Introduction

Un certain nombre de méthodes algorithmiques pour la résolution formelle d'équations algébriques sont devenues classiques et appartiennent au patrimoine de base du Calcul Formel. Parmi celles-ci, les algorithmes de bases standard et la méthode de Wu Wen-Tsün, occupent une place privilégiée. L'application de ces méthodes au cas des systèmes d'équations différentielles ordinaires ou aux dérivées partielles est beaucoup plus récente, bien que la méthode de Wu ne soit qu'un cas particulier de la théorie développée par Ritt en algèbre différentielle.

Les problèmes de complexité liés à ces algorithmes se présentent sous deux aspects différents : d'une part évaluer la complexité intrinsèque d'un problème dans le pire des cas, d'autre part isoler un certain nombre de cas particuliers non triviaux pour lesquels la complexité est acceptable. De telles études concourent soit au développement d'algorithmes plus performants, soit à un meilleur emploi des algorithmes existants, en se restreignant aux cas où ils peuvent se montrer efficaces.

La preuve de bornes de complexité requiert un appareillage théorique fin, et fournit en retour un éclairage nouveau sur la structure algébrique des objets calculés. En effet, l'expérience acquise montre une corrélation nette entre une bonne complexité et des propriétés algébriques simples.

Cette thèse tente, modestement, de se placer dans cette problématique, en proposant une étude transversale d'un problème ayant des applications pratiques, principalement en modélisation, sous le nom de *problème de l'identifiabilité structurelle globale*. D'un point de vue algébrique, il s'agit de tester si une fraction rationnelle appartient à un sous-corps du corps des fractions en n variables. On s'intéressera particulièrement au problème de tester si $k(f_1, \ldots, f_m) = k(x_1, \ldots, x_n)$. Un problème similaire est de tester si un polynôme appartient à une sous-algèbre de type fini de $k[x_1, \ldots, x_n]$.

Dans les deux cas, on pourra ramener le problème de multiples manières à la résolution d'un, ou de plusieurs systèmes d'équations algébriques, qui seront résolus soit par les algorithmes de base standard, soit par la méthode Wu–Ritt. Dans le cas polynomial, on dispose en outre d'une méthode intrinsèque, utilisant les algorithmes de bases canoniques, récemment introduits par Kapur et Madlener, et indépendamment par Robbiano et Sweedler.

Le problème de l'identifiabilité se résume de la manière suivante. On modélise un processus par une structure, décrite par un système d'équations différentielles, dépendant de fonctions de commande décrivant l'action de l'expérimentateur et d'un certain nombre de paramètres internes, qui sont des constantes physiques a priori inconnues. Des mesures, dépendant continûment de l'état du système sont effectuées. On les décrit de manière abstraite par des fonctions des variables d'état. Le problème est alors de savoir si, à partir d'une série d'expériences en nombre arbitrairement grand, on pourra déterminer de manière univoque les paramètres internes, sous l'hypothèse que ceux-ci sont génériques. En d'autres termes, il s'agit de vérifier que l'application qui associe à un n-uplet de paramètres le comportement entrée-sortie du système est injective sur un ouvert dense.

Un premier problème est de manipuler le comportement entrée-sortie. Des techniques classiques permettent de lui substituer une application polynomiale f équivalente, appelée résumé exhaustif. On teste alors que $k(f_1, \ldots, f_n) = k(x_1, \ldots, x_n)$, ce qui ramène au problème algébrique décrit ci-dessus. Nos travaux dans ce domaine se sont très largement inspirés des résultats antérieurs obtenus par LECOURTIER, RAKSANYI et WALTER au Laboratoire des Signaux et Systèmes à Supélec.

On introduira une mise en œuvre plus fine des techniques de résolution algébrique, qui permet un gain d'efficacité notable. Surtout, on étendra le calcul d'un résumé exhaustif à des structures non linéaires quelconques, sous quelques réserves de généricité, en employant les techniques d'algèbre différentielle, qui sont actuellement d'un emploi croissant en automatique, par exemple dans les travaux de Michel FLIESS.

Ce mémoire se compose de trois parties distinctes, d'un volume inégal, qui marquent les étapes conceptuelles de ce travail. La première donne des résultats théoriques préliminaires, regroupés en deux chapitres. Le premier est une introduction à l'algèbre différentielle, qui m'a paru indispensable pour fixer les notations et énoncer les propriétés de base utiles pour la suite. Le second traite des applications rationnelles et polynomiales, tant dans le cas algébrique que dans le cas différentiel. On y a réuni un certain nombre de résultats d'algèbre, difficiles, et qui auront leur importance pour l'algorithmique et l'étude de complexité.

Citons un théorème, prouvé par GABBER qui permet de majorer le degré de l'inverse d'un application birationnelle $f : \mathbf{A}^n \mapsto \mathbf{A}^n$ par $(\deg f)^{n-1}$. On donnera une version différente, qui se montre plus fine dans certains cas, et surtout un analogue dans le cas différentiel, permettant de borner l'ordre def^{-1} par $n \operatorname{ord} f$.

Le dernier paragraphe décrit des techniques permettant de ramener l'étude d'un sous-corps de $k(x_1, \ldots, x_n)$ ou d'une sous-algèbre à celle d'un idéal associé. La première utilise le graphe de l'application rationnelle associée à un ensemble de générateurs. Il s'agit donc d'une technique très classique et qui a déjà été beaucoup utilisée pour des applications effectives par VAN DEN ESSEN, SHANNON et SWEEDLER, etc. Une technique différente, moins connue, utilise une "section générique" du graphe. Elle apparaît chez RITT au cours de la démonstration d'un analogue différentiel du théorème de Lüroth. Les méthodes de LECOURTIER et RAKSANYI en sont assez proches, et je n'ai eu qu'à en préciser la signification géométrique.

La seconde partie traite des méthodes algorithmiques. Elles concernent principalement les méthodes de résolution de systèmes algébriques ou algébriques différentiels, qui permettent de mettre en action les traductions en termes d'idéaux décrites au chapitre II.

Le troisième chapitre débute par la description d'un "cadre général" pour les bases standard, mettant en relief les liens conceptuels qui unissent bases standard d'idéaux, bases canoniques et bases standard d'idéaux différentiels. Ce formalisme tient compte du fait que les bases standard généralisées à d'autres structures sont en général infinies (bases canoniques de sous-algèbres) et que l'ensemble des syzygies peut être lui-même infini (bases standard d'idéaux différentiels). On donne ensuite des algorithmes de résolution utilisant les bases standard classiques, rappelant la méthode du graphe et décrivant la méthode de section générique. On donne des bornes de complexité, simplement exponentielles, reposant soit sur le théorème de Gabber, soit sur le nullstellensatz effectif.

Le dernier paragraphe décrit les bases canoniques de sous-algèbres qui apparaissent clairement comme une généralisation des bases standard. On s'attachera surtout aux problèmes de finitude, conjecturant que la base canonique d'une sous-algèbre intégralement close et de type fini est finie, et aux applications aux automorphismes de $k[x_1, \ldots, x_n]$. On dispose dans ce cas d'une borne du même ordre, et même meilleure, ce que confirme l'expérience, qu'avec les méthodes utilisant un idéal associé.

Quelques relations entre bases canoniques et bases standard sont également présentées, comme une généralisation des bases standard aux idéaux d'une sous-algèbre, apparaissant comme un cas particulier d'une généralisation précédente de Sweedler et une méthode effective pour obtenir un système de générateurs de l'idéal des relations entre les éléments d'un base canonique, qui est une base standard pour un ordre bien choisi.

Le quatrième chapitre aborde les méthodes de résolution dans le cadre différentiel, commençant par une généralisation des bases standard, reprenant une notion précédemment introduite par Giuseppa Carra' Ferro. Précisons qu'elle est distincte de la théorie des bases standard de $\mathcal{D}$-modules. On y donne une procédure qui converge vers la base standard, sans qu'on soit sûr de pouvoir l'atteindre puisqu'elle est en général infinie. Dans quelques cas particuliers on peut néanmoins l'employer avec certitude, par exemple pour des idéaux isobares, où l'on retrouve les propriétés des bases standard d'idéaux homogènes. Dans le cas général, il faut disposer de bornes sur l'ordre de dérivation.

L'analogue différentiel du théorème de Gabber nous en fournit une, qui débouche sur une méthode algorithmique.

On décrit ensuite un algorithme de construction d'ensembles caractéristiques. Il faut noter qu'en général on ne sait pas construire l'ensemble caractéristique d'un idéal, fût-il premier, mais seulement un système d'ensembles caractéristiques dont certains — on ignore lesquels — définissent les composantes irréductibles de l'idéal. Cela suppose en outre de pouvoir factoriser des polynômes après plusieurs extensions algébriques du corps de base. Ne considérant que des idéaux premiers, j'ai pu remédier à cet inconvénient par une méthode qui suppose qu'on sait déjà tester l'appartenance à l'idéal, et nécessitant uniquement des décompositions sans facteur multiple.

Si l'on connaît déjà un ensemble caractéristique de l'idéal premier $\mathcal{I}$, le test d'appartenance nécessaire s'en déduit aisément et l'on peut alors tester qu'une application rationnelle $f : V(\mathcal{I}) \mapsto \mathbf{A}^m$ admet un inverse à gauche rationnel. Dans la mesure où les idéaux différentiels ne sont pas tous de type fini, et qu'il faut bien les définir par quelque chose, ce n'est pas une trop grande limitation que de le faire par un ensemble caractéristique, dont la connaissance est en général nécessaire, pour s'assurer au préalable que l'idéal est premier.

La dernière partie ne comporte, elle, qu'un chapitre décrivant les applications. Il commence par un rappel de quelques notions fondamentales et des résultats de LECOURTIER, RAKSANYI et WALTER. On donne ensuite une méthode originale pour le calcul des résumés exhaustifs dans le cas non-linéaire et des exemples d'applications. Cette méthode utilise l'élimination préalable des variables d'état, par un calcul d'ensemble caractéristique. N'ayant pas encore achevé l'implantation de cet algorithme, on ne pourra donner que des exemples susceptibles d'être calculés à la main, à titre d'illustration.

Par des méthodes reposant sur des techniques classiques de calculs de résumés exhaustifs, on donne un exemple résolu en 4 min. par Scratchpad II sur IBM 4381, alors que le programme de Raksanyi échoue par saturation de la mémoire après près d'une journée de calcul. Ce gain de temps ne peut s'expliquer uniquement par la puissance de l'ordinateur. Le calcul des bases standard est lent en Scratchpad II qui ne dispose en outre, dans cette configuration, que de 4M de mémoire disponible pour les calculs.

On trouvera en appendice le code Scratchpad II permettant de traiter les structures linéaires stationnaires, ainsi qu'une implantation d'un algorithme de construction de bases canoniques.

PREMIÈRE PARTIE

Approche théorique

CHAPITRE I

Algèbre différentielle

Dans ce chapitre, $\mathcal{F}$ désignera un corps différentiel simple ou aux dérivées partielles. On ne considérera que des anneaux et des corps commutatifs. On notera $\mathcal{F}^*$ le groupe des éléments inversibles de $\mathcal{F}$. Si E est un espace vectoriel, on notera $E_\star$ l'ensemble $E \setminus \{0\}$. Pour tout anneau intègre A, $\mathrm{Fr}A$ sera le corps de fractions de A.

§ 1. ANNEAUX DIFFÉRENTIELS

1. Définitions

DÉFINITION 1. — *Soit A un anneau, on appelle dérivation sur A une application $\delta : A \mapsto A$ telle que pour tout $(x, y) \in A^2$*

$$\delta(x+y) = \delta(x) + \delta(y) \tag{1}$$

$$\delta(xy) = x\delta(y) + y\delta(x). \tag{2}$$

On appelle anneau (resp. corps) différentiel un anneau (resp. un corps) muni d'un ensemble Δ de dérivations commutant entre elles, et anneau de Ritt un anneau différentiel contenant un sous-anneau isomorphe à $\mathbf{Q}$. *Lorsqu'on voudra faire explicitement référence à l'ensemble de dérivations considéré, on notera A_Δ. Dans le cas où il n'y a qu'une dérivation, on parlera d'un anneau différentiel ordinaire et autrement d'un anneau aux dérivées partielles.*

On notera Θ le monoïde commutatif libre engendré par les dérivations. Ses éléments seront appelés opérateurs de dérivation.

DÉFINITION 2. — *Soit A_Δ un anneau différentiel, on appelle module différentiel sur A_Δ, un A-module M muni d'un ensemble d'applications internes commutant entre elles Δ', en bijection avec Δ par ϕ, tel que*

$$\forall (x, y) \in M^2\ \forall \delta \in \Delta' \quad \delta(x+y) = \delta(x) + \delta(y)$$

et

$$\forall (a,x) \in A \times \mathrm{M}\, \forall \delta \in \Delta' \quad \delta(ax) = \phi(\delta)(a)x + a\delta(x).$$

Les applications de Δ' sont appelées dérivations sur M. On conviendra à l'avenir d'identifier Δ et Δ'.

On peut alors définir de manière immédiate les notions d'espace vectoriel différentiel, algèbre différentielle, etc.

DÉFINITION 3. — *Soit A un anneau différentiel, on appelle idéal différentiel de A, un sous-module différentiel de A considéré comme module différentiel sur lui-même, c'est donc en particulier un idéal algébrique.*

On s'assure aisément que les idéaux différentiels sont les idéaux $\mathcal{I}$ tels que $\Delta\mathcal{I} \subset \mathcal{I}$.

DÉFINITION 4. — *Soit A_Δ et $B_{\Delta'}$ deux anneaux différentiels, on appelle morphisme d'anneaux différentiels la donnée d'un morphisme d'anneaux $\phi : A \mapsto B$ et d'une bijection $\psi\colon \Delta \mapsto \Delta'$ tels que pour tout $(a,\delta) \in A \times \Delta$ $\phi(\delta\, a) = (\psi(\delta))\, \phi(a)$.*

Lemme 1. — Soit δ une dérivation d'un anneau différentiel A, alors $\delta\, 0 = 0$. Si A est unitaire, $\delta\, 1 = 0$.

PREUVE. $\delta\, 0 = \delta\,(0+0) = 2\,\delta\, 0$. $\delta\, 1 = \delta(1^2) = 2\,\delta\, 1$.

PROPOSITION 1. — *L'image d'un morphisme d'anneaux différentiels $\phi : A \mapsto B$ est un sous-anneau différentiel de B.*

Le noyau d'un morphisme d'anneaux différentiels est un idéal différentiel. Réciproquement, pour tout idéal différentiel Σ de A, l'anneau quotient A/Σ est canoniquement muni d'une structure d'idéal différentiel et Σ est le noyau du morphisme canonique de A dans A/Σ. ∎

PROPOSITION 2. — *Si E est un sous-ensemble d'un anneau différentiel A, il existe un unique idéal différentiel Σ contenant E qui soit minimal pour l'inclusion.*

PREUVE. Il suffit de prendre pour Σ l'intersection des idéaux contenant E. ∎

DÉFINITION 5. — *On appelle idéal différentiel engendré par E et l'on note $[E]$ le plus petit idéal différentiel contenant E.*

Lemme 2. — L'idéal différentiel $[E]$ est égal à l'idéal algébrique $(\Theta\, E)$. ∎

DÉFINITION 6. — *Un idéal différentiel $\mathcal{I}$ de A est dit radiciel [(1)], si*

$$\forall a \in A\, \exists n \in \mathbf{N}_\star\; a^n \in \mathcal{I} \implies a \in \mathcal{I}.$$

Lemme 3. — Si E est un sous-ensemble d'un anneau différentiel A, il existe un unique idéal différentiel radiciel contenant E, qui soit minimal pour l'inclusion.

PREUVE. Il suffit de prendre l'intersection des idéaux radiciels contenant E, en remarquant qu'il en existe au moins un, puisque $[1]$ est radiciel, et que l'intersection d'une famille d'idéaux radiciels est un idéal radiciel. ∎

---

(1) On dit aussi *parfait*, selon la terminologie de Ritt.

DÉFINITION 7. — *On appelle idéal radiciel engendré par un sous-ensemble E de l'anneau différentiel A, et l'on note $\{E\}$, le plus petit idéal radiciel contenant E.*

PROPOSITION 3. — *Si A est un anneau de Ritt, alors, pour tout idéal Σ de A, $\{\Sigma\} = \sqrt{\Sigma}$.*

PREUVE. On a manifestement $\sqrt{\Sigma} \subset \{\Sigma\}$. Pour prouver qu'on a l'inclusion inverse, il faut montrer que $\sqrt{\Sigma}$ est un idéal différentiel. Pour cela, il suffit de montrer que si a^n est dans Σ alors il existe une puissance de $\delta\, a$ dans Σ, ce qui résulte du lemme suivant. ∎

Lemme 4. — *Soient a un élément d'un anneau différentiel A et δ une dérivation de A, alors pour tout $n \in \mathbf{N}$ $(\delta\, a)^{2n-1} \in [a^n]$.*

PREUVE. Voir [Ri2 I.8 p. 8]. ∎

En particulier, un idéal différentiel premier est radiciel.

DÉFINITION 8. — *Soit $\mathcal{I}$ et $\mathcal{J}$ deux idéaux, on notera $\mathcal{I} : \mathcal{J}^\infty$ l'idéal $\{P \in \mathcal{F}\{n\} | \exists (a, Q) \in \mathbf{N} \times \mathcal{J}\ P\, Q^a \in \mathcal{I}\}$. On notera $\mathcal{I} : \Sigma^\infty$ l'idéal $\mathcal{I} : (\Sigma)^\infty$.*

Lemme 5. — *Si $\mathcal{I}$ est un idéal différentiel, alors $\mathcal{I} : \mathcal{J}^\infty$ est aussi un idéal différentiel.* ∎

2. Propriétés. Exemples

Tout anneau peut être muni d'une structure d'anneau différentiel triviale en prenant pour dérivation l'application nulle.

PROPOSITION 4. — *Soit A un anneau différentiel intègre et K son corps de fractions, alors il existe une unique dérivation sur K qui prolonge la dérivation de A. Elle est telle que $\delta(a/b) = \delta\, a/b - a\, \delta\, b/b^2$.*

PREUVE. Voir [ZS vol I ch. II § 17 p. 120]. ∎

En utilisant le lemme 1.1, on en déduit que la seule dérivation sur $\mathbf{Q}$ est la dérivation triviale.

THÉORÈME 1. — *Soit k un corps différentiel de caractéristique 0, alors pour toute extension algébrique K de k il existe une unique dérivation sur K qui prolonge la dérivation sur k.*

PREUVE. Voir [ZS vol. I ch. II § 17 cor. 2′ p. 125]. ∎

Exemples. — 1) L'anneau des polynômes (resp. le corps des fractions) en une variable est un anneau (resp. un corps) différentiel pour l'opération de dérivation usuelle. On voit que la dérivation sur le corps des fractions prolonge celle sur l'anneau.

2) L'anneau des polynômes (resp. le corps des fractions) en n variables x_i est un anneau (resp. un corps) différentiel pour chacune des n opérations de dérivation partielle $\frac{\partial}{\partial x_i}$.

3) Pour tout corps différentiel $\mathcal{F}$ de caractéristique 0, la clôture algébrique $\overline{\mathcal{F}}$ possède une unique structure de corps différentiel compatible avec celle de $\mathcal{F}$. En particulier, la seule dérivation sur la clôture algébrique de $\mathbf{Q}$ est la dérivation triviale. Par densité, on en déduit que c'est la seule dérivation continue sur $\mathbf{C}$ ou sur $\mathbf{R}$.

DÉFINITION 9. — *Si B est une algèbre différentielle sur A et E un sous-ensemble de B, la sous-algèbre différentielle engendrée par E sera notée $A\{E\}$. Si $\mathcal{G}$ est un sur-corps différentiel de $\mathcal{F}$, le sur-corps de $\mathcal{F}$ engendré par une partie η de $\mathcal{G}$ est noté $\mathcal{F}\langle\eta\rangle$.*

Lemme 6. — *Sous les hypothèses de la définition précédente,* $A\{E\} = A[\Theta\, E]$ *et* $\mathcal{F}\langle\eta\rangle = \mathcal{F}(\Theta\,\eta)$. ∎

§ 2. POLYNÔMES DIFFÉRENTIELS

1. Construction

On va définir les algèbres de polynômes différentiels sur un anneau différentiel A_Δ. Remarquons tout d'abord qu'on peut considérer des polynômes au sens usuel en une infinité de variables. Si S est un ensemble, on peut considérer $A[S]$ où A est un anneau comme la A-algèbre associée au monoïde $\mathbf{N}^{(S)}$ des applications à valeur dans $\mathbf{N}$ à support fini. On se donne maintenant un ensemble X de variables et l'on définit l'ensemble des dérivées $\Theta \times X$, que l'on notera Υ. L'élément (θ, x) de Υ sera noté $x_{(\theta)}$ et l'on définit une action de Θ sur Υ en posant $\theta'\, x_{(\theta)} = x_{(\theta'\theta)}$. L'ordre de l'opérateur de dérivation $\theta = \prod_{i=1}^{p} \delta_i^{\alpha_i}$ sera $\sum_{i=1}^{p} \alpha_i$, l'ordre de la dérivée $x_{(\theta)}$ sera l'ordre de θ. On notera $\operatorname{ord}\theta$ ou $\operatorname{ord} v$ l'ordre d'un opérateur de dérivation ou d'une dérivée.

On notera Θ_r l'ensemble des opérateurs différentiels d'ordre inférieur ou égal à r.

DÉFINITION 1. — *Soit A_Δ un anneau différentiel, X un ensemble, on appellera algèbre de polynômes différentiels sur A en les variables X l'algèbre $A[\Upsilon]$, qui sera notée $A\{X\}_\Delta$, ou $A\{X\}$ lorsqu'il n'y aura pas ambiguïté.*

On appellera monôme un produit de dérivées, et l'on notera $\mathcal{M}$ l'ensemble des monômes.

PROPOSITION 1. — *Soient A_Δ est un anneau différentiel, X un ensemble, il existe un unique ensemble Δ' d'opérations de dérivation sur $A\{X\}$ qui prolongent les dérivations de A et l'action de ces dérivations sur les dérivées, c'est à dire qu'identifiant Δ et Δ' on a bien $\delta(1.x_\theta) = 1.x_{\delta\theta}$.*

En outre, ces dérivations en font une algèbre différentielle sur A et satisfont pour tout polynôme $P = \sum_{i=1}^{p} c_i\, m_i$, où les m_i sont des monômes et les c_i des coefficients dans A,

$$\delta\, P = \sum_{i=1}^{p} \delta\, c_i\, m_i + \sum_{v\in\Upsilon} \frac{\partial\, P}{\partial\, v}\, \delta\, v.$$

PREUVE. Voir [BA V.16.1, prop. 1, p. 121]. ∎

Pour tout anneau A, l'anneau des polynômes en n variables est l'anneau $A\{[1,n]\}$, que nous noterons conventionnellement $A\{n\}$, ou $A\{x_1, \ldots, x_n\}$ selon l'usage, lorsque le besoin se fera sentir d'individualiser les variables. Suivant les notations de Ritt, on notera $x_{i,(j)}$ la $j^{\text{ème}}$ dérivée de x_i pour des polynômes différentiels ordinaires et, par exemple, $x_{j,(111233)}$ la dérivée partielle $\delta_1^3\delta_2\delta_3^2 x_j$.

DÉFINITION 2. — *Si $\mathcal{F}$ est un corps différentiel, on appelle corps des fractions différentielles en n variables, et l'on note $\mathcal{F}\langle n\rangle$ le corps des fractions de $\mathcal{F}\{n\}$ muni de la dérivation induite.*

Conventionnellement, si A est un anneau sans dérivation, on pourra le considérer comme un anneau différentiel avec un ensemble de dérivation vide. Idéaux différentiels et algébriques coïncident alors trivialement, ce qui permet alors d'identifier les notations (S) et $[S]$; on identifiera de même $A[X]$ et $A\{X\}$, $k(X)$ et $k\langle X\rangle$. D'une manière générale, pour énoncer des résultats strictement identiques dans le cas algébrique et dans le cas différentiel, on utilisera les notations du cas différentiel.

AVERTISSEMENT. — **L'algèbre différentielle, initiée par Ritt, est une théorie distincte de celle des anneaux d'opérateurs différentiels. Il importe en particulier de ne pas confondre l'anneau des polynômes différentiels sur $A\{n\}$ avec l'algèbre de Weyl $A[x_1,\ldots,x_n,\frac{\partial}{\partial x_1},\ldots\frac{\partial}{\partial x_n}]$.** Une différence essentielle, tant d'un point de vue théorique que pour les applications effectives, est que $A\{n\}$ est une A algèbre commutative, mais pas de type fini, tandis que l'algèbre de Weyl est non commutative mais de type fini.

2. Graduations admissibles

DÉFINITION 3. — *Soient $\nu_1,\ldots,\nu_n$ et $\mu_1,\ldots,\mu_m$ des réels positifs ou nuls, pour toute dérivée $v=\delta_1^{a_1}\cdots\delta_m^{a_m}x_i$, on définit $g_{\nu,\mu}(v)=\nu_i+\sum_{j=1}^m a_j\mu_j$. Pour un monôme $M=\prod_{i=1}^p v_i^{a_i}$, on définit $g_{\nu,\mu}(M)=\sum_{i=1}^p a_i\,g(v_i)$.*

Si $\mu=0$ et $\nu_i=1$, g correspond au degré. En prenant $\mu_i=1$ et $\nu=0$, on appellera g le poids. On notera $\mathrm{wt}\,P$ le poids maximal des monômes de P.

En désignant par A_r le sous-espace vectoriel — algébrique ! — engendré par les monômes M tels que $g(M)=r$, on obtient une graduation $\mathcal{F}\{n\}=\sum_{r\in g(\mathcal{M})}A_r$. Les graduations ainsi définies seront appelées graduations admissibles et les vecteurs ν et μ les systèmes de poids de la graduation. Les polynômes homogènes pour le poids seront dits isobares.

Une graduation différentielle est une graduation telle que $\delta A_r\subset A_r$.

Lemme 1. — *Une graduation admissible est différentielle ssi $\mu=0$.*

PREUVE. On s'assure aisément qu'il est nécessaire et suffisant, pour qu'une graduation soit différentielle, que $g\delta_i v=gv$ pour toute dérivée v. Or $g\delta_i v=gv+\mu_i$, d'où la conclusion. ∎

Lemme 2. — *Soit P un polynôme différentiel, homogène pour une graduation admissible g. Alors pour toute dérivation δ, δP est homogène pour g, ssi les coefficients de P appartiennent au corps des constantes de $\mathcal{F}$.*

PREUVE. Il suffit de vérifier que pour un terme $M=c\prod_{i=1}^p v_i^{\alpha_i}$, $\delta_j M$ est homogène de poids $g\,M+\mu_j$, ssi $\delta_j\,c=0$. ∎

PROPOSITION 2. — *Un idéal différentiel $\mathcal{I}$ engendré par un ensemble Σ de polynômes à coefficients constants et homogènes pour une graduation admissible g est gradué pour g.*

PREUVE. On a $\mathcal{I}=(\Theta\,\Sigma)$ et en utilisant le lemme précédent ont peut donc décomposer tout polynôme de $\mathcal{I}$ en une somme d'éléments de $\mathcal{I}$ homogènes. ∎

Remarques. — 1) Si la graduation est différentielle, il est clair que l'on n'a guère besoin de supposer que les coefficients des générateurs soient constants.

2) Si l'idéal $\mathcal{I}$ est homogène pour une graduation différentielle, alors $\{\mathcal{I}\}$ et ses composantes sont homogènes.

3) En caractéristique 0, si $P \notin \mathcal{F}$, $\mathrm{wt}\,\theta P = \mathrm{ord}\,\theta + \mathrm{wt}\,P$ $\theta \in \Theta$.

§ 3. GÉOMÉTRIE ALGÉBRIQUE DIFFÉRENTIELLE

1. Théorème de la base finie. Décomposition des idéaux radiciels

L'anneau différentiel $\mathcal{F}\{n\}$ n'est pas noetherien, même en ne considérant que les idéaux différentiels. Déjà en une variable, on peut montrer que les idéaux $\mathcal{I}_i = [x^2, \ldots, x_{(i)}^2]$ forment une chaîne d'idéaux emboîtés strictement croissante. Cependant, il existe une propriété de noetherianité pour l'ensemble des idéaux différentiels radiciels.

DÉFINITION 1. — *Un anneau de Ritt est dit radiciellement noetherien, si toute chaîne strictement croissante d'idéaux différentiels radiciels emboîtés est finie.*

THÉORÈME 1 (Théorème de la base finie de Ritt–Raudenbush). — *Soit A un anneau de Ritt, radiciellement noetherien, alors $A\{x\}$ est radiciellement noetherien.*

PREUVE. Voir [Ko2 chap. III § 4 th. 1 p. 126]. ■

COROLLAIRE 1. — *L'anneau $\mathcal{F}\{n\}$ est radiciellement noetherien.*

PREUVE. La preuve par récurrence est immédiate, en utilisant le théorème. ■

Lemme 1. — *Soit $\mathcal{I}$ un idéal radiciel de $\mathcal{F}\{n\}$, A et B deux polynômes tels que $AB \in \mathcal{I}$, alors $\mathcal{I} = \{\mathcal{I}, A\} \cap \{\mathcal{I}, B\}$.*

PREUVE. L'inclusion de gauche à droite est immédiate. Soit P dans $\{\mathcal{I}, A\} \cap \{\mathcal{I}, B\}$, $P^a = M + NA$ avec $M \in \mathcal{I}$ et $P^b = M' + N'B$ avec $M' \in \mathcal{I}$. En multipliant ces égalités membre à membre, on trouve $P^{a+b} = MM' + N'BM + NAM' + NN'AB \in \mathcal{I}$. Donc P appartient à $\mathcal{I}$. ■

THÉORÈME 2. — *Soit $\mathcal{I}$ un idéal radiciel de $\mathcal{F}\{n\}$, il existe un unique ensemble fini E d'idéaux premiers tel que*

$$\mathcal{I} = \bigcap_{\Omega \in E} \Omega$$

et

$$\forall (\Omega, \Omega') \in E^2 \quad \Omega \subset \Omega' \implies \Omega = \Omega'.$$

PREUVE. Supposons le théorème faux. En utilisant le cor. 1 du théorème de la base finie de Ritt-Raudenbush, on peut alors trouver un idéal radiciel $\mathcal{I}$ de $\mathcal{F}\{n\}$ ne vérifiant pas la conclusion et maximal. $\mathcal{I}$ n'est pas premier. Soient A et B deux polynômes tels que $AB \in \mathcal{I}$, $A \notin \mathcal{I}$ et $B \notin \mathcal{I}$. Alors $\{\mathcal{I}, A\}$ et $\{\mathcal{I}, B\}$ admettent une décomposition comme intersection finie d'idéaux premiers, sinon $\mathcal{I}$ ne serait pas maximal. Comme d'après le lemme 1, $\mathcal{I} = \{\mathcal{I}, A\} \cap \{\mathcal{I}, B\}$, $\mathcal{I}$ se décompose en une intersection finie d'idéaux premiers.

On peut alors retirer de l'ensemble de ces idéaux tous ceux qui sont inclus dans un autre. On obtient bien un ensemble vérifiant la conclusion du théorème. Soit maintenant deux ensembles d'idéaux premiers S et S' vérifiant la conclusion. Alors, pour tout $\Omega \in S$, il existe $\Omega' \in S'$ tel que $\Omega \subset \Omega'$ et il existe de même $\Omega'' \in S$ tel que $\Omega' \subset \Omega''$. On en déduit $\Omega = \Omega''$ et donc $\Omega = \Omega'$, ce qui assure l'unicité. ■

2. Variétés. Composantes

Avant de définir des variétés algébriques différentielles, il est nécessaire de se livrer à quelques préliminaires. RITT définissait la variété associée à un ensemble de polynômes algébriques différentiels comme la classe de ses zéros, sur toutes les extensions possibles du corps de base. Mais ceci ne constitue pas un ensemble. KOLCHIN a remédié à cet inconvénient (cf. [Ko1]) en montrant qu'on pouvait se restreindre à prendre des zéros dans une extension universelle (cf. [Ko2 chap. III § 7 p.133]), notion que nous allons introduire.

Cette présentation, quelque peu technique offre une sorte d'analogue de la clôture algébrique, mais il s'agit en fait d'un objet beaucoup plus grand. On peut également le définir dans le cas algébrique, en prenant un ensemble de dérivations vide ; il a alors, comme dans le cas différentiel un degré de transcendance infini par rapport au corps de base.

DÉFINITION 2. — *Soit $\mathcal{I}$ un idéal de $\mathcal{F}\{n\}$, on appelle zéro de $\mathcal{I}$ un doublet $(\mathcal{G}, \eta)$, où $\mathcal{G}$ désigne une extension de $\mathcal{F}$ et η un élément de $\mathcal{G}^n$, tel que $P(\eta) = 0$ pour tout polynôme P de $\mathcal{I}$. On appelle zéro générique de $\mathcal{I}$ un zéro $(\mathcal{G}, \eta)$ tel que $\{P \in \mathcal{F}\{n\} | P(\eta) = 0\} = \mathcal{I}$.*

Lemme 2. — Tout idéal premier $\mathcal{I}$ de $\mathcal{F}\{n\}$ admet un zéro générique.

PREUVE. Comme $\mathcal{I}$ est premier, l'anneau différentiel $\mathcal{F}\{n\}/\mathcal{I}$ est intègre. Soit $\mathcal{G}$ son corps de fractions. On peut prendre pour zéro générique $(\mathcal{G}, \eta)$ où η_i désigne l'élément de $\mathcal{G}$ associé à x_i par le morphisme canonique de $\mathcal{F}\{n\}$ dans $\mathcal{G}$. ■

DÉFINITION 3. — *indeExtension universelle Soit $\mathcal{F}$ un corps différentiel, on appelle extension universelle de $\mathcal{F}$ une extension $\mathcal{U}$ telle que pour toute extension finie $\mathcal{F} \subset \mathcal{G} \subset \mathcal{U}$ tout entier $n > 0$ et tout idéal $\mathcal{I} \neq \{1\}$ de $\mathcal{G}\{n\}$, il existe un zéro générique de $\mathcal{I}$ dans $\mathcal{U}$.*

PROPOSITION 1. — *Si $\mathcal{U}$ est une extension universelle de $\mathcal{F}$, $\mathcal{U}$ est une extension universelle de toute extension finie de $\mathcal{F} \subset \mathcal{G} \subset \mathcal{U}$.*

PREUVE. Voir [Ko2 p. 133] ■

PROPOSITION 2. — *Si $\mathcal{U}$ est une extension universelle de $\mathcal{F}$, $\mathcal{U}$ est algébriquement clos et son corps des constantes est un corps algébriquement clos contenant la clôture algébrique du corps des constantes de $\mathcal{F}$.* ■

THÉORÈME 3 (Kolchin). — *Tout corps différentiel admet une extension universelle.*

PREUVE. Voir [Ko2 p. 134]. ■

Remarque 1. — Il n'est pas gênant que l'extension universelle ne soit pas unique. En effet, il suffit d'en choisir une et de la conserver. Par définition même, on n'aura jamais besoin d'une extension plus grande. D'autre part, la démonstration de Kolchin construit pour tout corps $\mathcal{F}$ une extension universelle définie de manière unique.

Ces préliminaires permettent de définir les variétés algébriques différentielles. Cette construction, bien que nécessaire pour travailler en toute rigueur, est sans grande conséquence sur le fond. À part le fait qu'elle permet de recourir à des éléments génériques, ce qui est parfois commode, elle nous ramène surtout à travailler avec des idéaux premiers, les composantes associées n'en étant que le reflet.

Par la suite on supposera choisie une extension universelle $\mathcal{U}$ de $\mathcal{F}$.

DÉFINITION 4. — *Soit Σ un sous-ensemble de $\mathcal{F}\{m\}$, on appelle variété algébrique différentielle associée à Σ l'ensemble $V(\Sigma)$ des zéros des polynômes de Σ dans une extension universelle de $\mathcal{F}$, qui seront appelés les points de la variété.*

On appellera espace affine différentiel de dimension p sur $\mathcal{F}$, et l'on notera $\mathbf{A}^p_{\mathcal{F}}$, l'ensemble des zéros de l'idéal $[0]_{\mathcal{F}\{p\}}$, c'est-à-dire $\mathcal{U}^p$.

Donnons quelques propriétés élémentaires des variétés algébriques différentielles (par la suite, nous dirons seulement variété, lorsqu'il n'y aura pas d'ambiguïté). Elles généralisent exactement la situation algébrique.

PROPOSITION 3. — *L'intersection de deux variétés algébriques V_1 et V_2 définies par $\mathcal{I}$ et $\mathcal{I}'$ est une variété algébrique définie par $\mathcal{I}+\mathcal{I}'$. L'union de V_1 et V_2 est elle aussi une variété, définie par $\mathcal{I}\cap\mathcal{I}'$.* ■

THÉORÈME 4 (Théorème des zéros). — *Soit V une variété définie par un sous-ensemble Σ de $\mathcal{F}\{n\}$, alors l'ensemble $\{P \in \mathcal{F}\{n\} | \forall \eta \in V\, P(\eta) = 0\}$ est un idéal radiciel de $\mathcal{F}\{n\}$, égal à $\{\Sigma\}$.*

PREUVE. Voir [Ko2 chap IV § 2 p. 146].

DÉFINITION 5. — *On appelle variété irréductible, une variété qui ne peut pas s'exprimer comme réunion de deux variété non vides.*

COROLLAIRE 1. — *Toute variété V peut s'exprimer comme une réunion finies de variétés irréductibles, qu'on appellera les composantes de V.*

PREUVE. Soit $\mathcal{I}$ l'idéal radiciel définissant V, $\mathcal{I}$ peut se décomposer en une intersection finie d'idéaux premiers $\mathcal{I}_i$ définissant chacun une variété irréductible V_i. V est manifestement égal à la réunion des V_i. ■

COROLLAIRE 2. — *Tout idéal $\mathcal{I} \neq \{1\}$ définit une variété algébrique non vide.*

PREUVE. Si $\mathcal{I}$ est différent de $\{1\}$, $\mathcal{I}$ s'exprime comme intersection finie d'idéaux premiers tous différents de $\{1\}$. Chacun d'entre eux admet un zéro générique, qui est aussi un zéro de $\mathcal{I}$. ■

3. Espace projectif

DÉFINITION 6 (Espace projectif, variétés projectives). — *Soit $\mathcal{F}$ un corps différentiel, $\mathcal{U}$ une extension universelle de $\mathcal{F}$, on appellera espace projectif de dimension p sur $\mathcal{F}$, $\mathbf{P}_p$, l'ensemble des classes d'équivalence de $\mathcal{U}^{p+1} \setminus \{0\}$ par la relation identifiant les $p+1$-uplets multiples l'un de l'autre.*

On appellera variété différentielle projective, l'ensemble $V(\Sigma)$ des classes d'équivalence des zéros dans $\mathcal{U}^{p+1} \setminus \{0\}$ d'un ensemble de polynômes homogènes Σ de $\mathcal{F}\{p+1\}$. Ces classes d'équivalences seront appelées les points de la variété projective. L'ensemble Σ sera dit définir la variété.

On identifiera $\mathbf{A}^p_{\mathcal{F}}$ avec l'ensemble des éléments de $\mathbf{P}_p$ dont les représentants ont une première coordonnée non nulle, qui seront dits *points à distance finie*.

Lemme 3. — *L'ensemble des polynômes qui s'annulent sur tous les représentants des classes d'équivalence formant une variété projective différentielle V, définie par un idéal homogène $\mathcal{J}$, est un idéal différentiel radiciel homogène $\mathcal{I}$ définissant V. On notera cet idéal $\mathcal{I}(V)$. L'idéal $\mathcal{I} \cap \mathcal{J}$ définit également la variété.*

PREUVE. Cet ensemble est manifestement un idéal. Soit un polynôme $P \in \mathcal{I}$ de degré d, on peut le décomposer en une somme de polynômes homogènes P_i de degré i. Comme on est en caractéristique 0, on peut trouver $d+1$ constantes a_j distinctes et non nulles dans $\mathcal{F}$. L'ensemble des classes de V est invariant par multiplication par un élément non nul, donc $P(a_j x) \in \mathcal{I}$ $j \in [1, d]$. Comme a_j est une constante $P(a_j x) = \sum_{i=1}^{d} a_j^i P_i$. Par un argument classique d'algèbre linéaire, on conclut que les P_i appartiennent à $\mathcal{I}$. Donc $\mathcal{I}$ est homogène.

Pour s'assurer que $\mathcal{I}$ définit bien V, il suffit de vérifier que l'ensemble W constitué des représentants de V et de l'origine forme une variété différentielle algébrique affine. $\mathcal{I}$ est un idéal dans $\mathcal{F}\{x_0, \ldots, x_n\}$; prenons une variable supplémentaire y et considérons l'idéal $\mathcal{I}' = [P(y\,x_0, \ldots, y\,x_n) | P \in \mathcal{I}] : (y)^\infty$ dans $\mathcal{F}\{X, y\}$. W est manifestement la variété définie par $\mathcal{I}' \cap \mathcal{F}\{X\}$.

Le fait que $\mathcal{I} \cap \mathcal{J}$ définisse V est immédiat puisque $V(\mathcal{J}) \subset W$. ∎

Remarques. — 1) Cette définition contient en particulier le cas algébrique pur en prenant un ensemble de dérivation vide.

2) Contrairement au cas différentiel affine, ou au cas algébrique projectif, il n'y a plus bijection entre les idéaux radiciels homogènes et les variétés projectives. Il suffit de considérer l'idéal $[x_0']$ dans $\mathcal{F}\{x_0, x_1\}$, manifestement premier, mais dont les classes des zéros constituent $\mathbf{P}_1$ tout entier.

Lemme 4. — *Soient G le groupe d'automorphismes de $\mathcal{U}\{n+1\}$ $\{g_a : P(x) \mapsto P(a\,x) | x \in \mathcal{U}^*\}$, $\mathcal{J}$ un idéal différentiel premier homogène de $\mathcal{F}\{n+1\}$, alors la variété projective V définie par $\mathcal{J}$ est égale à la variété projective définie par l'idéal $\mathcal{J}_G = \{P \in \mathcal{J} | \forall g \in G\, gP \in [\mathcal{J}]_{\mathcal{U}\{n+1\}}\}$. Cet idéal est premier et égal à $\mathcal{I}(V)$.*

PREUVE. On s'assure aisément que G est un groupe et $\mathcal{J}_G$ un idéal. Il est immédiat que les représentants des classes de $\mathcal{J}$ sont des zéros de $\mathcal{J}_G$. Donc $\mathcal{J}_G \subset \mathcal{I}(V)$. Soient $P \notin \mathcal{J}_G$ un polynôme de $\mathcal{J}$, $(\eta_0, \ldots, \eta_n)$ un zéro générique de $\mathcal{J}$, pour tout élément non nul a de $\mathcal{F}$,

$a\eta$ est un représentant d'un zéro de la variété. On peut choisir a tel que $g_a\, P \notin [\mathcal{J}]_{\mathcal{U}\{n+1\}}$, mais dans ce cas P ne s'annule pas sur $a\eta$. Donc $\mathcal{I}(V) \cap \mathcal{J} \subset \mathcal{J}_G$. D'après le lemme 3, V est bien la variété définie par $\mathcal{J}_G$.

Montrons que$\mathcal{J}_G$ est premier. Soit $PQ \in \mathcal{J}_G$, pour a générique sur $\mathcal{F}$, $g_a P$ ou $g_a Q$ appartiennent à l'ideal

$$[\mathcal{J}]_{\mathcal{F}\langle a\rangle\{n+1\}} = \mathcal{F}\langle a\rangle\, \mathcal{J} = [\mathcal{J}]_{\mathcal{U}\{n+1\}} \cap \mathcal{F}\langle a\rangle\{n+1\},$$

car cet idéal est premier par généricité de a. On en déduit que P ou Q appartiennent à $\mathcal{J}_G$. L'égalité de $\mathcal{J}_G$ et $\mathcal{I}(V)$ est alors immédiate. ∎

DÉFINITION 7. — *Un variété projective V sera dite irréductible si $\mathcal{I}(V)$ est premier. Un point générique d'une variété irréductible est un point admettant un représentant qui est un zéro générique de $\mathcal{I}(V)$.*

PROPOSITION 4. — *Soit V une variété différentielle, il existe un unique ensemble fini $\{\mathcal{I}_1, \ldots, \mathcal{I}_r\}$ d'idéaux radiciels premiers stables par G et disjoints entre eux, tels que $\mathcal{I} = \bigcap_{i=1}^r \mathcal{I}_i$.*

PREUVE. Soit $\mathcal{J}$ un idéal définissant V. Utilisant le th. 1.2 p. 8, on peut decomposer $\{\mathcal{J}\}$ en $\bigcap_{i=1}^s \mathcal{J}_i$ où les $\mathcal{J}_i$ sont premiers. Utilisant le lemme 4, $\mathcal{I}(V) = \bigcap_{i=1}^s \mathcal{I}_{j\,G}$ et il suffit d'éliminer ceux des idéaux qui sont strictement inclus dans un autre. ∎

COROLLAIRE 1. — *Il y a bijection entre les variétés différentielles projectives irréductibles et les idéaux premiers homogènes stables par G. Plus généralement, il y a bijection entre les variétés différentielles projectives et les idéaux radiciels stables par G.*

Pour toute variété projective V définie par un idéal $\mathcal{J}$, $\mathcal{I}(V) = \{\mathcal{J}_G\} = \{\mathcal{J}\}_G$.

PREUVE. La première partie est une conséquence immédiate du lemme 4.

Utilisant la proposition, on décompose $\mathcal{I}(V) = \bigcap_{i=1}^s \mathcal{I}_i$. Puis, on procède comme pour la démonstration du lemme 4. Soit η_i un zéro générique de $\mathcal{I}_i$. Il est aisé de voir que si $P \notin \mathcal{J}_G$, il existe $a \in \mathcal{U}^*$ et η_i tel que $g_a\, P(\eta_i) \neq 0$. Donc $\mathcal{I}(V) \cap \mathcal{J} \subset \mathcal{J}_G$. D'autre part, pour tout $P \in \mathcal{J}_G$, tout η_i et tout $a \in \mathcal{U}^*$, $g_a\, P(\eta_i) = 0$, donc $\mathcal{J}_G \subset \mathcal{I}(V)$. Utilisant le lemme 3, $\mathcal{J}_G$ définit donc la variété V. En fait, on a même mieux, car d'après la démonstration de ce lemme $\mathcal{J}_G$ défini la variété affine W correspondant à l'ensemble des représentants des points de V. On en déduit donc que $\mathcal{I}(V) = \{\mathcal{J}_G\}$.

Pour prouver que $\mathcal{I}(V) = \{\mathcal{J}\}_G$, il suffit de montrer que cet idéal, qui définit lui aussi W, est radiciel. Supposons que $(g_a\, P)^r \in \mathcal{J}' = [\{\mathcal{J}\}]_{\mathcal{U}\{n+1\}}$. Comme $\{\mathcal{J}\}$ est radiciel et qu'on est en caractéristique 0, $\mathcal{J}'$ est également radiciel (voir [ZS vol. II th. 37 p. 226]). Donc $g_a\, P \in \mathcal{J}'$.

Ceci montre bien la correspondance biunivoque entre idéaux radiciels stables par G et les variétés algébriques différentielles projectives. ∎

On peut achever par deux lemmes faciles, laissés au lecteur, nécessaires pour compléter notre “outillage”.

Lemme 5. — *Si V est une variété projective dans $\mathbf{P}_p$ admettant des points à distance finie, alors un point de V est un point générique ssi c'est un point générique de $V \cap \mathbf{A}^p$.* ∎

Lemme 6. — *Soit V une variété projective de $\mathbf{P}_p$, on obtient un idéal définissant $V \cap \mathbf{A}^p$ en évaluant x_0 à 1 et toutes les dérivées propres de x_0 à 0 dans $\mathcal{I}(V)$.* ∎

Par la suite, on entendra par variété différentielle algébrique une variété affine ou projective.

4. Topologie de Zariski différentielle

PROPOSITION 5. — *Soit V une variété différentielle, affine ou projective, on définit un topologie sur V, en prenant comme fermés les sous-variétés de V.*

PREUVE. Voir [Ko2 chap IV § 1], où le cas affine est traité. Le cas projectif s'en déduit immédiatement, en remarquant que $V \cap W$ est la variété définie par $\mathcal{I}(V) + \mathcal{I}(W)$ (2). ∎

On appellera cette topologie la *topologie de Zariski différentielle.*

Lemme 7. — *Soient V une variété différentielle, η un point de V, alors η est dense dans V ssi V est irréductible et η est générique.* ∎

PROPOSITION 6. — *Soit V une variété projective de $\mathbf{P}_n$ définie par un idéal $\mathcal{I}$ de $\mathcal{F}\{x_0, \ldots, x_n\}$, la projection de V sur $\mathbf{P}_p$ est une variété projective définie par l'idéal $\mathcal{I} \cap \mathcal{F}\{x_0, \ldots, x_p\}$.*

Si V est une variété affine de $\mathbf{A}^n$, l'adhérence de Zariski de la projection de V sur $\mathbf{A}^p$ est définie par $\mathcal{I} \cap \mathcal{F}\{x_1, \ldots, x_p\}$. ∎

DÉFINITION 8. — *Soit P un polynôme de $\mathcal{F}\{x_1, \ldots, x_n\}$, on appelle homogénéisé de P et l'on note $\widetilde{P}$ le numérateur de la fraction réduite $P(x_1/x_0, \ldots, x_n/x_0)$ dans $\mathcal{F}\langle x_0, \ldots, x_n\rangle$.*

Si $P \in \mathcal{F}\{x_0, \ldots, x_n\}$ est un polynôme homogène, on appellera déshomogénéisé de P le polynôme obtenu en évaluant x_0 à 1 dans P. On le note $\widehat{P}$.

Lemme 8. — *Soit $\mathcal{I}$ un idéal de $\mathcal{F}\{n\}$ et V la variété affine qu'il définit, l'adhérence dans $\mathbf{P}_n$ de V est définie par $\widetilde{\mathcal{I}}$. Si Σ est un ensemble de polynômes définissant V, la variété projective définie par $\widetilde{\Sigma}$ contient l'adhérence projective de V.*

Si V est une variété projective de $\mathbf{P}_n$, $V \cap \mathbf{A}^n$ est définie par l'idéal $\widehat{\mathcal{I}}(V)$. ∎

DÉFINITION 9. — *On appellera couple de polynômes pertinent sur une variété différentielle V, un couple (P, Q) de polynômes homogènes et de même degré tels que $\forall a \in \mathcal{F}^*$ $P(a\,x)Q(x) - Q(a\,x)P(x) \in \mathcal{I}(V)$.*

DÉFINITION 10. — *Soit V une variété différentielle affine, une fonction f de V dans $\mathcal{F}$ est dite régulière en un point η de V si elle est définie en η, s'il existe un couple (P, Q) de polynômes et un voisinage ouvert $\mathcal{O}$ de η tel que $\mathcal{O} \subset V \setminus V(Q)$ et $f_{|\mathcal{O}} = P/Q$.*

Si V est une variété projective, f de V dans $\mathcal{F}$ est régulière en un point η s'il existe un voisinage ouvert $\mathcal{O}$ de η et un couple (P, Q) pertinent tels que tout point de $\mathcal{O}$ admette un représentant $\epsilon \in \mathcal{U}^{n+1}$ avec $Q(\epsilon) \neq 0$ et tels que $f_{|\mathcal{O}} = P/Q$.

(2) En revanche il est en général faux que $\mathcal{J}_1 + \mathcal{J}_2$ définissent $V \cap W$ si $\mathcal{J}_1$ et $\mathcal{J}_2$ sont deux idéaux homogènes définissant les variétés projectives V et W.

Remarques. — 1) Pour que P et Q satisfassent $P(a\,x)/Q(a\,x) = P(x)/Q(x)$, il est nécessaire mais non suffisant qu'ils soient homogènes et de même degré, à moins qu'on ne soit sur un corps de constantes, ou que P et Q soient d'ordre 0.

2) Pour tous polynômes P et Q, notant d_1 et d_2 leurs degrés respectifs, d le maximum de ces degrés, P' et Q' les polynômes $\widetilde{P}\,x_0^{d-d_1}$ et $\widetilde{Q}\,x_0^{d-d_2}$, on a :

$$P'(a\,x)Q'(x) - Q'(a\,x)P'(x) = 0\ \forall a \in \mathcal{F}.$$

Lemme 9. — *Si (P, Q) et (R, S) sont pertinents par rapport à $\mathcal{I}$, $(\delta\,P\,Q + P\,\delta\,Q, Q^2)$, $(PS + RQ, QS)$ et (PR, QS) sont pertinents.*

PREUVE. Comme

$$\begin{aligned}&P(ax)R(ax)S(x)Q(x) - P(x)R(x)S(ax)Q(ax) =\\&\quad (P(ax)Q(x) - P(x)Q(ax))R(ax)S(x) + (R(ax)S(x) - R(x)S(ax))P(x)Q(ax) \in \mathcal{I},\end{aligned}$$

(PR, QS) est pertinent. On s'assure aisément que pour tout polynôme P (P, P) est pertinent, donc il suffit de vérifier que si (P, Q) et (R, Q) sont pertinents, $(P + R, Q)$ est pertinent, ce qui résulte alors d'un calcul aisé. D'autre part,

$$\begin{aligned}&(\delta\,P(ax)\,Q(ax) - P(ax)\,\delta\,Q(ax))Q^2(x) - (\delta\,P(x)\,Q(x) - P(x)\,\delta\,Q(x))Q^2(ax) =\\&\delta(P(ax)\,Q(x) - P(x)\,Q(ax))Q(x)Q(ax) + (P(x)\,Q(ax) - P(ax)\,Q(x))(\delta\,Q(ax)Q(x) + \delta\,Q(x)Q(ax)) \in \mathcal{I},\end{aligned}$$

d'où l'on conclut que le couple exprimant la dérivée par δ est pertinent. ∎

DÉFINITION 11. — *On appelle corps de fonctions d'une variété algébrique différentielle irréductible V non vide, les classes d'équivalences de doublets $(f, \mathcal{O})$, où f est une fonction à valeurs dans $\mathcal{F}$ régulière sur l'ouvert $\mathcal{O}$ de V, obtenues en identifiant $(f, \mathcal{O})$ et $(g, \mathcal{O}')$ si f et g coïncident sur $\mathcal{O} \cap \mathcal{O}'$. On le note $\mathbf{K}(V)$.*

Si V est une variété différentielle affine irréductible, définie par un idéal premier $\mathcal{I}$ on appellera anneau de coordonnnées de V l'anneau $\mathcal{F}\{n\}/\mathcal{I}$ qui sera noté $A(V)$.

Le fait que $\mathbf{K}(V)$ soit un corps est immédiat si V est affine. Dans le cas projectif, c'est une conséquence directe du lemme précédent. Ce corps est manifestement une extension différentielle finie de $\mathcal{F}$, isomorphe dans le cas affine au corps des fractions de $A(V)$.

N'ayant pas trouvé de références pour un espace projectif différentiel, il m'a fallu développer cette notion dans la mesure où elle présente quelques difficultés techniques qui n'apparaissent pas dans le cadre algébrique. On dispose maintenant d'un matériel suffisant. Presque tous les résultats classiques sur les morphismes de variétés algébrique (cf. [Ha chap. I § 3]) s'étendent aux variétés différentielles. Il faut cependant souligner une différence notable, bien qu'elle soit sans grande conséquence dans la suite de notre étude.

Remarque 3. — Dans le cas algébrique, l'ensemble des fonctions $f\colon V \mapsto \mathcal{F}$, régulières en tout point d'une variété affine coïncide avec l'anneau de coordonnées de V. Ce n'est plus vrai pour une variété algébrique différentielle. Il suffit de considérer $V = V(x' - x)$ et $f = 1/(x - 1)$.

DÉFINITION 12. — *On notera $\mathcal{O}(V)$ l'anneau des fonctions régulières en tout point d'une variété algébrique différentielle V.*

Soient X et Y deux variétés algébriques différentielles, V un ouvert de X on appellera morphisme de V dans Y une application $\phi: V \mapsto Y$, continue pour la topologie de Zariski, et telle que pour tout ouvert $\mathcal{O}$ de Y et toute fonction f régulière sur $\mathcal{O}$, $f \circ \phi: \phi^{-1}(\mathcal{O}) \mapsto \mathcal{F}$ est régulière.

On pourra se reporter à l'article [Car2] de Giuseppa CARRA'-FERRO pour plus de détails et des références plus complètes.

§ 4. APPROCHE COMBINATOIRE

1. Ensembles caractéristiques

Les définitions qui vont suivre sont à la base de la méthode effective de RITT–WU. Nous les retrouverons au chapitre IV d'un point de vue plus effectif, mais il est utile de les donner ici afin d'énoncer certains résultats théoriques. On considère une algèbre de polynômes différentiels sur un corps différentiel $\mathcal{F}_\Delta$ de caractéristique 0, avec un ensemble fini de variables $X = \{x_1, \ldots, x_n\}$. On désignera par m le cardinal de Δ. On reprend ici la présentation et les notations de [Ko2], avec des renvois aux démonstrations. Dans la mesure où l'anneau de base est un corps de caractéristique 0, on peut simplifier en modifiant certaines définitions. On donnera alors des démonstrations explicites si les objets ne coïncident pas exactement.

On rappelle qu'on note Θ le monoïde des opérateurs engendré par Δ, et $\Upsilon = \Theta X$ l'ensemble des dérivées.

DÉFINITION 1. — *On dira qu'un ordre $<$ sur Υ est admissible si $v < v' \implies \theta v < \theta v'$ et si $v \leq \theta v$.*

PROPOSITION 1. — *Tout ordre admissible sur Υ est un bon ordre, c'est à dire que toute chaîne décroissante d'élément de Υ est stationnaire à partir d'un certain rang.*

PREUVE. Voir [Ko2 chap. 0 § 17 lemme 15 p. 49].

DÉFINITION 2. — *Soit $v = x_{i,(\theta)}$ une dérivée, on appelle classe de v l'indice i de la variable correspondante.*

On va définir un ordre admissible sur Υ, d'autres seront donnés au chapitres IV.

DÉFINITION 3. — *Θ est isomorphe au monoïde $\mathbf{N}^m$, on l'ordonne en choisissant un ordre admissible pour la structure de monoïde, qui respecte le degré, c'est-à-dire ici l'ordre de dérivation, par exemple l'ordre lexicographique inverse. On définit alors un ordre sur Υ, en posant*

$$x_{i,(\theta)} < x_{i',(\theta')} \iff \begin{array}{l}\theta < \theta' \\ \text{ou } \theta = \theta' \textit{ et } i < i'.\end{array}$$

Cet ordre sera appelé ordre différentiel, provenant de l'ordre choisi sur Θ

On s'assure aisément que cet ordre est admissible. Par la suite, on suppose qu'un ordre admissible $<$ a été choisi, et l'on va l'étendre en un préordre sur les polynômes différentiels.

Définition 4. — *On dit qu'un ordre admissible respecte l'ordre de dérivation si* $\operatorname{ord} \upsilon > \operatorname{ord} \nu \implies \upsilon > \nu$.

On s'assure aisément que si l'ordre sur Θ respecte l'ordre de dérivation, alors l'ordre différentiel sur Υ aussi.

Définition 5. — *Soit $P \notin \mathcal{F}$ un polynôme différentiel, on appelle dérivée dominante de P et l'on note υ_P la plus grande dérivée intervenant dans P. L'ordre et la classe de P seront ceux de υ_P. Dans ce contexte, le degré de P sera son degré en υ_P. On obtient un préordre sur $\mathcal{F}\{X\}_\star$ prolongeant $<$ en posant $P \leq Q$ si*

A) $P \in \mathcal{F}$,

B) $P, Q \notin \mathcal{F}$ et $\upsilon_P < \upsilon_Q$,

C) $P, Q \notin \mathcal{F}$, $\upsilon_P = \upsilon_Q$ et $\deg P \leq \deg Q$.

On conviendra de noter $P < Q$ si $P \leq Q$ et $Q \not\leq P$ et $P \cong Q$ si $P \leq Q$ et $Q \leq P$.

Si $P \in \mathcal{F}^*$, on posera $\deg P = 0$ et $\deg P = -1$ si $P = 0$.

Considérant P comme un polynôme dans $\mathcal{F}[\nu < \upsilon_P][\upsilon_P]$. On appelle initial de P le coefficient dominant de P et séparant de P $\frac{\partial P}{\partial \upsilon_P}$. On les notera I_P et S_P.

Remarque 1. — Pour tout opérateur de dérivation $\theta \neq 1$ $S_P = I_{\theta P}$.

Définition 6 (Réduction). — *Soient P et $Q \notin \mathcal{F}$ deux polynômes de $\mathcal{F}\{X\}$, P est dit partiellement réduit par rapport à Q si P ne contient aucune dérivée stricte de υ_Q, et réduit par rapport à Q s'il est partiellement réduit et si $\deg_{\upsilon_Q} P < \deg Q$. Si $Q \in \mathcal{F}^*$, P est réduit par rapport à Q si $P = 0$. Dans le cas contraire, on dira que P est irréductible.*

On dira que P est réduit par rapport à un sous-ensemble Σ de $\mathcal{F}\{X\}$ si P est réduit par rapport à chacun de ses éléments.

Définition 7 (Ensemble autoréduit). — *On appelle ensemble autoréduit de $\mathcal{F}\{n\}$, un ensemble de polynômes non nuls Σ, éventuellement vide, tel que pour tout $P \in \Sigma$, P est réduit par rapport à $\Sigma \setminus \{P\}$.*

Proposition 2. — *Tout ensemble autoréduit de polynômes de $\mathcal{F}\{X\}$ est fini.*

preuve. Voir [Ko2 chap. I § 9 p. 77] ∎

On va étendre $\leq$ en un préordre sur les ensembles autoréduits — un singleton est manifestement un ensemble autoréduit — de la manière suivante.

Définition 8. — *Soientt $\mathcal{A} = \{A_1, \ldots, A_r\}$ et $\mathcal{B} = \{B_1, \ldots, B_s\}$ deux ensembles autoréduits non vides, où les polynômes sont supposés donnés par ordre croissant. On posera $\mathcal{A} < \mathcal{B}$ si*

i) il existe $k \leq \min(r, s)$ tel que $A_i \cong B_i$ pour $i < k$ et $A_k < B_k$, ou si

ii) $r > s$ et $A_i \cong B_i$ pour $i \leq s$.

Par convention, $\emptyset > \mathcal{A}$, pour tout $\mathcal{A}$ autoréduit non vide. Si $r = s$ et $A_i \cong B_i$ $i \leq r$, on notera $\mathcal{A} \cong \mathcal{B}$. On posera $\mathcal{A} \leq \mathcal{B}$, si $\mathcal{A} < \mathcal{B}$ ou si $\mathcal{A} \cong \mathcal{B}$.

On s'assure aisément que ceci définit bien un préordre.

Proposition 3. — *Dans tout ensemble E d'ensembles autoréduits, il existe un élément minimal pour ce préordre.*

preuve. Voir [Ko2 chap. I § 10 p. 81] ∎

DÉFINITION 9 (Ensemble caractéristique). — *Soit $\mathcal{I}$ un idéal différentiel de $\mathcal{F}\{n\}$, on appelle ensemble caractéristique de $\mathcal{I}$ un ensemble autoréduit minimal parmi les ensembles autoréduits constitués d'éléments de $\mathcal{I}$.*

Lemme 1. — *Si $\mathcal{A}$ est un ensemble caractéristique d'un idéal $\mathcal{I}$, pour tout polynôme A de $\mathcal{A}$, I_A et S_A n'appartiennent pas à $\mathcal{I}$.*

PREUVE. Il est aisé de voir que I_A et S_A sont non nuls et réduits par rapport à $\mathcal{A}$. Si l'un d'eux appartenait à $\mathcal{I}$, on pourrait former un ensemble autoréduit d'éléments de $\mathcal{I}$ plus petit que $\mathcal{A}$ en lui adjoignant les éléments de $\mathcal{A}$ qu'il ne réduit pas. ∎

PROPOSITION 4. — *Soient $\mathcal{A} = \{A_1, \ldots, A_r\}$ un ensemble autoréduit, et P un polynôme différentiel de $\mathcal{F}\{X\}$, alors il existe un polynôme différentiel P_0, réduit par rapport à $\mathcal{A}$ et des entiers $\alpha_1, \ldots, \alpha_r$ et $\beta_1, \ldots, \beta_r$ tels que*

$$\left(\prod_{i=1}^{r} (I_{A_i})^{\alpha_i} \, (S_{A_i})^{\beta_i}\right) \, P - P_0 = \sum_{j=1}^{s} M_j \, \theta_j \, A_{i_j},$$

où $\theta_1 \, A_{i_1} \leq P$ et $\theta_j \, A_{i_j} > \theta_{j'} \, A_{i_{j'}}$ si $j > j'$. On notera alors $P \xrightarrow{\mathcal{A}} P_0$.

PREUVE. Ceci résultera d'un algorithme de réduction qui sera détaillé au chapitre IV. On peut aussi se reporter à [Ko2 chap I § 9 p. 79]. ∎

PROPOSITION 5. — *Si $\mathcal{A}$ est un ensemble caractéristique d'un idéal $\mathcal{I}$ de $\mathcal{F}\{n\}$, alors pour tout polynôme P de $\mathcal{I}$, $P \xrightarrow{\mathcal{A}} 0$.*

Si $\mathcal{I}$ est premier, alors pour tout polynôme P de $\mathcal{F}\{X\}$, $P \in \mathcal{I}$ ssi $P \xrightarrow{\mathcal{A}} 0$.

PREUVE. D'après la prop. 1, toute chaîne de réductions est finie, donc $P \xrightarrow{\mathcal{A}} P_0$, où P_0 est réduit par rapport à $\mathcal{A}$. Comme $P_0 \in \mathcal{I}$, si P_0 était non-nul, on pourrait comme dans la démonstration du lemme 1, obtenir un ensemble caractéristique plus petit que $\mathcal{A}$, ce qui est impossible.

Si $P \xrightarrow{\mathcal{A}} 0$, on a donc $(\prod_{i=1}^{r} I_{A_i}^{\alpha_i} \, S_{A_i}^{\beta_i}) \, P \in [\mathcal{A}]$, ce polynôme appartient donc également à $\mathcal{I}$. Si $\mathcal{I}$ est premier, en utilisant le lemme 1, on conclut que $P \in \mathcal{I}$. ∎

DÉFINITION 10. — *Soit C un sous-ensemble de $\mathcal{R}$, on appelle pseudo-syzygies entre éléments de C les couples $(\theta \, P, \theta' \, Q)$ où P et Q appartiennent à C, (θ, θ') sont deux éléments de $\Theta \setminus \{1\}$, $v_{\theta P} = v_{\theta' Q}$ et θ, θ' sont sans facteur commun. Le S-polynôme associé à une pseudo-syzygie est le polynôme $(S_Q/\mathrm{pgcd}(S_P, S_Q))\theta P - (S_P/\mathrm{pgcd}(S_P, S_Q))\theta' Q$.*

Si tous les S-polynômes associés aux syzygies entre éléments de C sont réduits à 0 par C, C est dit cohérent.

PROPOSITION 6. — *Soit C un sous-ensemble autoréduit et cohérent de $\mathcal{R}$, c'est un ensemble caractéristique d'un idéal premier $\mathcal{I}$ de $\mathcal{R}$ ssi notant v_C l'ensemble des dérivées qui apparaissent dans les éléments de C et H_C le produit des initiaux et des séparants des polynômes de C, l'idéal $(C) : H_C^\infty$ de $\mathcal{F}[v_C]$ est premier et aucun élément non nul de cet idéal n'est réduit par rapport à C.*

Dans ce cas, $\mathcal{I} = [C] : H_C^\infty$.

PREUVE. Voir [Ko2 chap IV § 9 lemme 2 p. 167]. ∎

COROLLAIRE 1. — *Soit P un polynôme premier de $\mathcal{F}\{n\}$, il forme un ensemble caractéristique d'un idéal premier égal à $[P] : (I_P S_P)^\infty$, qu'on appellera la composante générale de P.* ∎

2. Fonction et polynôme de transcendance

Un idéal algébrique premier se voit attacher deux invariants privilégiés, la dimension et le degré. La situation est analogue dans le cas différentiel où l'on considérera la dimension et l'ordre.

DÉFINITION 11. — *Soit $\mathcal{F}$ un corps différentiel, $\mathcal{G}$ une extension de $\mathcal{F}$ et η un élément de $\mathcal{G}$. On dit que η est différentiel sur $\mathcal{F}$, s'il existe un polynôme non nul P de $\mathcal{F}\{1\}$, tel que $P(\eta) = 0$. $\mathcal{G}$ est une extension différentielle de $\mathcal{F}$ si tous les éléments de $\mathcal{G}$ sont différentiels sur $\mathcal{F}$.*

DÉFINITION 12. — *Une famille $A = (\eta_i\ i \in [1, n])$, finie ou infinie, de polynômes de $\mathcal{G}$ est dite différentiellement liée sur $\mathcal{F}$, s'il existe un polynôme P de $\mathcal{F}\{n\}$ et une sous famille finie $\eta_1, \ldots, \eta_n$ de A tels que $P(\eta) = 0$, et différentiellement libre dans le cas contraire.*

THÉORÈME 1. — *Soit $\mathcal{G}$ une extension de $\mathcal{F}$ et $R \subset S$ deux sous-ensembles de $\mathcal{G}$ tels que R forme une famille différentiellement libre et que $\mathcal{G}$ soit différentiel sur $\mathcal{F}\langle S\rangle$, alors il existe un ensemble T tel que $R \subset T \subset S$, différentiellement libre et telle que $\mathcal{G}$ soit différentiel sur $\mathcal{F}\langle T\rangle$.*

De plus, si T est fini, toute famille libre T' telle que $\mathcal{G}$ est différentiel sur $\mathcal{F}\langle T'\rangle$ est finie et a même nombre d'éléments que T, et si T est infini, toute famille de ce type est infinie.

PREUVE. Voir [Ko2 chap II § 9 th. 4 p 105]. ∎

DÉFINITION 13. — *Soit $\mathcal{G}$ une extension finie de $\mathcal{F}$, on appelle degré de transcendance différentiel de $\mathcal{G}$ sur $\mathcal{F}$ le cardinal d'une famille différentiellement libre T telle que $\mathcal{G}$ soit différentiel sur $\mathcal{F}\langle T\rangle$.*

Si $\mathcal{I}$ est un idéal premier de $\mathcal{F}\{n\}$, on appelle dimension de $\mathcal{I}$ le degré de transcendance différentiel du corps de fractions $\mathcal{F}\{n\}/\mathcal{I}$ sur $\mathcal{F}$. Si V est une variété sur $\mathcal{F}$, sa dimension est le degré de transcendance différentiel de son corps de fonctions $\mathbf{K}(V)$ sur $\mathcal{F}$.

Remarques. — 1) Contrairement au cas algébrique, la dimension d'une variété différentielle ne coïncide pas en général avec sa dimension topologique. Par exemple, la dimension de la variété définie par $[x_{(11)}, x_{(22)}]_{\mathbf{Q}\{x\}_{\delta_1,\delta_2}}$ est 0, tandis que sa dimension topologique, qui coïncide ici avec le degré de transcendance algébrique de son corps de fonctions, est 4.

2) Si V est une sous-variété projective de $\mathbf{P}_n$ d'intersection non vide avec $\mathbf{A}^n$, la dimension de V est égale à celle de $V \cap \mathbf{A}^n$.

3) Pour tout zéro générique η de $\mathcal{I}$, la dimension de $\mathcal{I}$ est aussi le degré de transcendance de $\mathcal{F}\langle\eta\rangle$ sur $\mathcal{F}$. En effet, il est aisé de voir que pour tout zéro générique η de $\mathcal{I}$, $\mathcal{F}\langle\eta\rangle$ est isomorphe à $\mathrm{Fr}\mathcal{F}\{n\}/\mathcal{I}$.

DÉFINITION 14. — *Soit $\mathcal{F}\langle\eta\rangle$ une extension de $\mathcal{F}$, on appelle fonction de transcendance de η sur $\mathcal{F}$, la fonction notée $H_{\eta/\mathcal{F}}$ telle que $H_{\eta/\mathcal{F}}(r)$ soit égal au degré de transcendance algébrique de $\mathcal{F}(\Theta_r\,\eta)$ sur $\mathcal{F}$.*

PROPOSITION 7. — *Pour r assez grand, la fonction de transcendance $H_{\eta/\mathcal{F}}$ est égale à un polynôme*

$$\omega_{\eta/\mathcal{F}}(r) = \sum_{i=1}^{m} a_i \binom{i+r}{i}.$$

L'entier a_m est égal au degré de transcendance différentiel de $\mathcal{F}\langle\eta\rangle$ sur $\mathcal{F}$.

PREUVE. Voir [Ko2 chap. II § 12 th. 6 p. 115] ■

On appellera ce polynôme le *polynôme de transcendance* de η sur $\mathcal{F}$.

PROPOSITION 8. — *Si $\mathcal{F}\langle\eta\rangle$ est isomorphe à $\mathcal{F}\langle\epsilon\rangle$, il existe un entier h tel que $\omega_{\eta/\mathcal{F}}(r-h) \leq \omega_{\epsilon/\mathcal{F}}(r) \leq \omega_{\eta/\mathcal{F}}(r+h)$.*

Si $\mathcal{F}(\eta)$ est isomorphe à $\mathcal{F}(\epsilon)$, η et ϵ ont même polynôme de transcendance.

Si $\mathcal{F}\langle\eta\rangle \subset \mathcal{F}\langle\epsilon\rangle$, $\omega_{\eta/\mathcal{F}} \leq \omega_{\epsilon/\mathcal{F}}$.

PREUVE. Voir [Ko2 chap. II § 12 prop. 15 p. 117] ■

DÉFINITION 15. — *Avec les notations de la propriété précédente, on appellera type de l'extension $\mathcal{F}\langle\eta\rangle$ sur $\mathcal{F}$, et l'on notera $\tau_{\eta/\mathcal{F}}$, le plus grand indice i tel que a_i soit non nul. L'entier $a_{\tau_{\eta/\mathcal{F}}}$ sera la dimension différentielle typique [Ko2] de l'extension.*

Enfin, suivant Ritt ([Ri2 chap. II et IV]), on appellera ordre de l'extension l'entier a_j avec $j = \max\{i < m | a_i \neq 0\}$ si cet ensemble est non vide, ou sinon 0.

Si $\mathcal{I}$ est un idéal premier et V la variété affine irréductible définie par $\mathcal{I}$, on étend naturellement ces définitions à $\mathcal{I}$ ou à V en considérant un zéro générique η de V.

Remarque 4. — L'ordre et la dimension différentielle typique coïncident si le type est inférieur à m, c'est-à-dire si l'on est en dimension 0.

3. Ensembles caractéristiques et fonctions de transcendance

On sait déterminer la fonction de Hilbert d'un idéal algébrique, dès lors qu'on en connaît une base standard. Les ensembles caractéristiques jouent un rôle analogue en algèbre différentielle, puisqu'ils permettent de déterminer la fonction de transcendance.

PROPOSITION 9. — *Soient $\mathcal{I} \neq [1]$ un idéal différentiel premier de $\mathcal{F}\{n\}$ de fonction de transcendance H, $\mathcal{A}$ un ensemble caractéristique de $\mathcal{I}$ pour un ordre qui respecte l'ordre de dérivation. On identifie l'ensemble Υ des dérivées avec $[1, n] \times \mathbf{N}^m$, et l'on note E l'ensemble des dérivées — propres ou non — des dérivées dominantes des polynômes de $\mathcal{A}$, I le complémentaire de cet ensemble. Le nombre de points de $I \cap [1, n] \times [0, r]^m$ est égal à $H(r)$.*

PREUVE. On trouvera la preuve complète dans [Ko2 chap. II § 12 th. 6 p. 115]. On peut remarquer que $\Theta\, E = E$, de sorte que E est la réunion de n escaliers dans $\mathbf{N}^m$, autant qu'il y a de variables. On obtient la fonction de transcendance $H(r)$ en comptant le nombre de points sous les escaliers d'ordre inférieur ou égal à r. La dimension de $\mathcal{I}$ correspond au nombre des variables pour lesquelles l'escalier est vide. ■

COROLLAIRE 1. — *Si P est un polynôme premier, l'ordre de la composante principale de P est égal à l'ordre de P* ■

PROPOSITION 10. — *Soient P un polynôme premier de $\mathcal{F}\{n\}$ d'ordre r, V la variété correspondant à la composante générale de P et $H_1, \ldots, H_{n-1}$ des hyperplans génériques de $\mathbf{A}^n_{\mathcal{F}}$, i.e. des hyperplans définis par $H_i = V([\epsilon_{i,0} + \sum_{j=1}^n \epsilon_{i,j} x_j])$, où les $\epsilon_{i,j}$ sont génériques sur $\mathcal{F}$. Alors, la variété $V \cap \bigcap_{i=1}^{n-1} H_i$ est irréductible, son type est $m-1$ et son ordre est r.*

PREUVE. Pour un ordre respectant l'ordre de dérivation et tel que $x_n > \cdots > x_1$, il existe un ensemble caractéristique $\mathcal{A}$ de l'idéal définissant l'intersection des hyperplans de la forme $\{x_2 - a_2 x_1 - b_2, \ldots, x_n - a_n x_1 - b_n\}$, où les a_i et b_i sont génériques sur $\mathcal{F}$. Réduire P par cet ensemble caractéristique, dont les initiaux et séparants valent 1, revient à y substituer $a_i x_1 + b_i$ à x_i pour $n \geq i > 1$. On obtient alors un polynôme $P'(x_1)$, premier, de même ordre que P. On note $\mathcal{B}$ l'ensemble $\mathcal{A} \cup \{P\}$, qui est manifestement autoréduit.

Montrons que $(\mathcal{B})$ est premier. Prenant pour variables les érivées qui apparaissent dans les polynômes de $\mathcal{B}$, on commence par remarquer que $\mathcal{B}$ forme une base standard algébrique pour tout ordre tel que $x_{1,(\theta)} < x_j$, car les monômes de tête sont étrangers. Soient R_1 et R_2 deux polynômes tels que $R_1 R_2 \in (\mathcal{B})$. On peut commencer à réduire (au sens des bases standard !) $R_1 R_2$ par $\mathcal{A}$, ce qui donne un reste $R'_1(x_1) R'_2(x_1)$. Comme $R_1 R_2$ se réduit à 0, $R'_1 R'_2 = M(x_1) P'$. Comme P' est irréductible, R'_1 ou R'_2 sont des multiples de P' donc réduits à 0 par $\mathcal{B}$ ce qui montre que R_1 ou R_2 sont dans $(\mathcal{B})$.

Plus généralement, le même raisonnement montre que tout polynôme R de $(\mathcal{B})$ s'exprime sous la forme

$$R = M_1(x_1) P' + \sum_{i=2}^{n} M_i(x_1, \ldots, x_i)(x_i - a_i x_1 - b_i),$$

donc est réductible par B au sens de la réduction de Ritt (déf. 1.6 p. 16). En dernier lieu, $\mathcal{B}$ est cohérent, car l'ensemble des pseudo-syzygies qui lui est associé est manifestement vide. On peut donc appliquer la prop. 1.6 p. 17 et conclure que $\mathcal{B}$ est un ensemble caractéristique de l'idéal premier $\mathcal{J} = [\mathcal{B}] : (\mathcal{I}_{\mathcal{P}'} \mathcal{S}_{\mathcal{P}'})^\infty$.

Il reste à prouver l'égalité entre $V(\mathcal{J})$ et $V \cap \bigcap H_i$. Soit η un zéro générique de $\mathcal{J}$. C'est un zéro de $\mathcal{A}$ et de P. Mais, comme $I_P \xrightarrow{\mathcal{B}} I_{P'} \notin \mathcal{J}$, ce n'est pas un zéro de I_P. Raisonnant de même pour le séparant, on en déduit que η est un zéro de $[\mathcal{A}] + [P] : (I_P S_P)^\infty$. Par généricité de η, $V(\mathcal{J}) \subset V \cap \bigcap H_i$

Réciproquement, soit ϵ un zéro d'une composante de $V \cap \bigcap H_i$. C'est donc un zéro de $\mathcal{A}$ et de P. Comme les $a_2, \ldots, a_n, b_2, \ldots, b_n$ forment une famille générique sur $\mathcal{F}$, ϵ est un zéro générique de P donc n'annule ni I_P, ni S_P. D'autre part, $I_P(\epsilon) = I_{P'}(\epsilon_1)$ et $S_P(\epsilon) = S_{P'}(\epsilon_1)$, d'où l'on déduit que ϵ n'annule ni $I_{P'}$ ni $S_{P'}$, et donc que c'est un zéro de $V(\mathcal{J})$, ce qui assure l'inclusion inverse.

On a donc montré que $\mathcal{B}$ est un ensemble caractéristique de l'idéal premier définissant la variété irréductible $V \cap \bigcap H_i$.

Il suffit maintenant d'appliquer la proposition 9 ci-dessus pour trouver que le polynôme de transcendance de $\mathcal{J}$ est égal à

$$\binom{m+r}{m} - \binom{m+r-\operatorname{ord} P}{m} = \operatorname{ord} P \binom{m-1+r}{m-1} + O\left(r^{(m-2)}\right). \quad \blacksquare$$

On dispose d'un théorème important, dû à RITT dans le cas différentiel ordinaire, qui le considérait comme l'analogue différentiel du théorème de BÉZOUT ; il permet de borner l'ordre d'un idéal premier à partir de l'ordre des dérivées intervenant dans chacun de ses générateurs. Il a été partiellement étendu par KOLCHIN au cas des idéaux aux dérivées partielles.

THÉORÈME 2 (Ritt–Kolchin). — *Soient $\mathcal{I}$ une composante de type $m-1$ de l'idéal $\{\Sigma\}$ de $\mathcal{F}\{n\}$, $e_i = \max\{\mathrm{ord}_{x_i} | P \in \Sigma\}$, alors l'ordre de Σ pour tout ensemble de variables arbitraires est borné par $\sum_{i=1}^{n} e_i$.*

PREUVE. Voir [Ko2 chap. IV § 17 prop. 9 p. 199]. ■

Dans le cas où les polynômes sont d'ordre nul, on a un résultat plus précis.

PROPOSITION 11. — *Si $\mathcal{I}$ est un idéal de $\mathcal{F}\{n\}$ engendré par un ensemble Σ de polynômes d'ordre nuls, alors, le polynôme de transcendance différentiel de $\mathcal{I}$ est égal à $d\binom{m+r}{m}$, où d désigne la dimension de l'idéal algébrique $(\Sigma)_{\mathcal{F}[n]}$.*

PREUVE. Voir [Ko2 chap. IV § 17 prop. 10 p. 200]. ■

Ce résultat n'est finalement qu'une manière plus précise de formuler le théorème 1.2.1 p 5.

CHAPITRE II

Inversibilité et appartenance à un sous-corps

Dans ce chapitre, $\mathcal{F}$ désignera un corps différentiel de caractéristique nulle, ou algébrique de caractéristique quelconque. On notera $\mathcal{F}\langle n\rangle$ le corps des fractions rationnelles en n variables $\mathcal{F}\langle x_1, \ldots, x_n\rangle$ et $\mathcal{F}\{n\}$ l'algèbre $\mathcal{F}\{x_1, \ldots, x_n\}$.

On précisera algébrique ou différentiel si des résultats diffèrent dans les deux situations.

§ 1. APPLICATIONS POLYNOMIALES ET RATIONNELLES

1. Définitions

Pour clarifier les idées et la terminologie, nous reprenons quelques définitions et propriétés élémentaires.

DÉFINITION 1. — *Soit $X \subset \mathbf{A}^n$ et $Y \subset \mathbf{A}^m$ deux variétés, on appelle application polynomiale de X dans Y toute application f définie par*

$$f(x) = (P_1(x), \ldots, P_m(x)),$$

où les P_i sont des polynômes de $\mathcal{F}\{n\}$.

DÉFINITION 2. — *Soit $X \subset \mathbf{A}^n$ (resp. $X \subset \mathbf{P}_n$) et $Y \subset \mathbf{A}^m$ (resp. $Y \subset \mathbf{P}_m$) deux variétés, on appelle application rationnelle une classe d'équivalence de doublets (U, ϕ_U), où U est un ouvert non vide de $\mathbf{A}^n$ (resp. $\mathbf{P}_n$) et ϕ un morphisme de U dans Y, définie en identifiant (U, ϕ_U) et (V, ϕ_V) si ϕ_U et ϕ_V coïncident sur $U \cap V$.*

Remarques. — 1) On voit qu'à toute application polynomiale g, on peut associer une application rationnelle, définie comme la classe de (g, X). On identifiera systématiquement toute application polynomiale avec l'application rationnelle associée.

2) Considérant $\mathbf{A}^n$ comme un ouvert de $\mathbf{P}_n$, toute application rationnelle entre deux variétés affines induit une unique application rationnelle entre leurs adhérences projectives. De même, toute application rationnelle entre deux variétés projectives X et Y se restreint en une application rationnelle entre $X \cap \mathbf{A}^n$ et $Y \cap \mathbf{A}^m$ pourvu que $Y \cap \mathbf{A}^m$ soit non vide.

PROPOSITION 1. — *Il y a une bijection entre les applications rationnelles de $X \subset \mathbf{A}^n$ dans $Y \subset \mathbf{A}^m$ et les m-uplets $(f_1, \ldots, f_m)$ de $\mathbf{K}(X)$ tels que pour tout P appartenant à $\mathcal{I}(Y)$ $P(f) = 0$.*

Pour toute application rationnelle projective $f\colon X \subset \mathbf{P}_n \mapsto Y \subset \mathbf{P}_m$, il existe un $(m+1)$-uplet de polynômes homogènes et de même degré $(f_0, \ldots, f_m)$, tels que tous les couples (f_i, f_j) soient pertinents, que l'un au moins des f_i n'appartienne pas à $\mathcal{I}(X)$, que $P(f) = 0$ pour tout polynôme de $\mathcal{I}(Y)$ et que

$$f(x_0, \ldots, x_n) = (f_0(x), \ldots, f_m(x)).$$

Réciproquement, tout $(m+1)$-uplet de polynômes satisfaisant ces conditions définit une application rationnelle de X dans Y. ■

Lemme 1. — *Soit $f\colon X \mapsto Y$ une application rationnelle affine définie par les m fractions f_i, ou une application projective définie par $m+1$ polynômes f_i, soit $\mathcal{J} = \{P \mid P(f) = 0\}$, alors $\mathcal{J}$ est un idéal premier et pour tout représentant (U, ϕ_U) de f l'adhérence de Zariski de ϕ_U est égale à $V(\mathcal{J})$.*

Pour tout point générique η de X, $f(\eta)$ est un point générique de l'adhérence de ϕ_U.
■

DÉFINITION 3. — *On appellera image d'une application rationnelle $f : X \mapsto Y$ la variété définie comme l'adhérence de l'image d'un de ses représentants.*

On dira que f est dominante si $Y = \mathrm{Im}(f)$.

La cohérence de cette définition résulte du lemme ci-dessus. On voit que toute application rationnelle peut être considérée comme une application dominante en restreignant la variété d'arrivée à la variété image.

Lemme 2. — *Soit f une application rationnelle sur X, V l'ouvert de X correspondant à la réunion des ouverts U pour tous les doublets (U, ϕ_U) définissant f, alors il existe un doublet (V, ϕ_V) définissant f.* ■

DÉFINITION 4. — *On appelle domaine de définition de f et l'on note* $\mathrm{Dom}(f)$, *la réunions des ouverts U pour tous les représentants (U, ϕ_U) de f, et fonction associée a f, la fonction définie sur le domaine de f et coïncidant avec $\phi_{\mathrm{Dom}(f)}$.*

Remarques. — 3) Une application rationnelle n'est pas véritablement une application, mais on peut la considérer comme une fonction définie sur un ouvert dense.

4) Si une application rationnelle projective est définie par $m+1$ polynômes f_i tels que f_0 n'est pas dans l'idéal définissant X, f induit une application rationnelle affine définie par les fractions $f_i(1, x_1, \ldots, x_n)/f_0(1, x_1, \ldots, x_n)$.

Réciproquement, si f est une application rationnelle affine définie par m fractions P_i/Q_i, l'application projective associée est définie par

$$(x_0, \ldots, x_n) \mapsto \left(\prod_{i=1}^{m} \widetilde{Q}_i x_0^{D-\Sigma_{i=1}^n \deg Q_i}, \widetilde{P}_1 x_0^{D-\deg P_1}, \ldots, \widetilde{P}_n x_0^{D-\deg P_n}\right),$$

où $\widetilde{P}$ désigne l'homogénéisé de P par la variable x_0 et $D = \max(\sum_{i=1}^n \deg Q_i, \max(\deg P_i))$.

2. Ordre et degré d'une application rationnelle

DÉFINITION 5. — *Soit $f\colon \mathbf{A}^n \mapsto \mathbf{A}^m$ une application rationnelle définie par des fractions réduites f_i, on appelle ordre de f le maximum des ordres des numérateurs et dénominateurs des f_i. Si $f\colon \mathbf{P}_n \mapsto \mathbf{P}_m$ est une application rationnelle, on appelle ordre de f le minimum des ordres des $(m+1)$-uplets de polynômes définissant f, l'ordre d'un i-uplet étant le maximum des ordres de ses polynômes.*

On s'assure aisément que ces définitions ne dépendent pas du repère choisi.

Remarque 1. — Si f est une application affine, les constructions de la remarque 1.4 montrent que son ordre est celui de l'application de projective associée.

DÉFINITION 6. — *Soit $f\colon \mathbf{P}_n \mapsto \mathbf{P}_m$ une application rationnelle, on appelle degré de f le minimum des degré des $m+1$-uplets définissant f. Le degré d'une application $f\colon \mathbf{A}^n \mapsto \mathbf{A}^m$ est le degré de l'application projective associée.*

Remarque 2. — Si $f\colon \mathbf{A}^n_{\mathcal{F}_\Delta} \mapsto \mathbf{A}^m_{\mathcal{F}_\Delta}$ est une application d'ordre 0, elle induit une application $f'\colon \mathbf{A}^n_{\mathcal{F}_\emptyset} \mapsto \mathbf{A}^m_{\mathcal{F}_\emptyset}$ de même degré que f. Cette application sera appelée *application rationnelle algébrique associée à f.*

3. Composition et applications inversibles

Si f est une application rationnelle dominante de W dans X et g une application rationnelle de X dans Y, on peut définir la composée $g \circ f$ de f et g. L'ensemble des applications dominantes d'une variété X dans elle-même forme un monoïde pour la composition, l'élément unité étant la classe de l'identité. La composition peut également être définie si g est polynomiale, où d'une manière plus générale s'il existe un représentant de g défini sur un ouvert U tel que $U \cap \mathrm{Im}(f) \neq \emptyset$.

DÉFINITION 7. — *On dit qu'une application f de X dans Y est rationnellement (resp. polynomialement) inversible si f admet un inverse rationnel (resp. polynomial) à gauche. Si f admet un inverse à droite et à gauche, on dit qu'elle est birationnelle et si f et f^{-1} sont polynomiales, on dit que f est bipolynomiale.*

Dans le cas affine, $\mathbf{K}(X)$ s'identifie naturellement à l'ensemble des applications rationnelles de X dans $\mathbf{A}^1$. À toute application f de X dans Y on peut donc associer l'application de $\mathbf{K}(Y)$ dans $\mathbf{K}(X)$ qui à ρ associe $\rho \circ f$.

THÉORÈME 1. — *La construction ci-dessus définit une bijection entre l'ensemble des applications rationnelle de X dans Y et les morphismes de $\mathbf{K}(Y)$ dans $\mathbf{K}(X)$. Une application f est birationnelle ssi le morphisme associé f^{tr} est un isomorphisme.*

Elle est inversible à gauche ssi $\mathbf{K}(\mathrm{Im}\, f)$ est isomorphe à $\mathbf{K}(X)$ par f^{tr}.

PREUVE. Voir [Ha] (l'extension au cas différentiel est immédiate). ∎

Remarques. — 1) Si f est affine, définie par des fractions f_i de $\mathbf{K}(X)$, l'inversibilité à gauche de f revient à l'égalité entre les corps $\mathbf{K}(X)$ et $\mathcal{F}\langle f\rangle$.

2) Dans le cas ou $f\colon \mathbf{A}^n \mapsto \mathbf{A}^m$ est d'ordre 0, elle est inversible ssi l'application algébrique associée est inversible, ce qui est équivalent à $\mathcal{F}(f_1,\ldots,f_m) = \mathcal{F}(x_1,\ldots,x_n)$. En particulier, si f est inversible d'ordre 0, l'ordre de f^{-1}est 0.

Dans le cas affine, on peut identifier l'anneau de coordonnées de X avec l'ensemble des applications polynomiales de X dans $\mathbf{A}^1$. On peut donc associer à toute application polynomiale de X dans Y un morphisme f^{tr}de $A(Y)$ dans $A(X)$.

THÉORÈME 2. — *Cette construction définit une bijection entre l'ensemble des applications polynomiales de X dans Y et les morphismes de $A(Y)$ dans $A(X)$. Une application f est bipolynomiale ssi le morphisme associé f^{tr} est un isomorphisme. Elle est polynomialement inversible à gauche ssi $A(\mathrm{Im}\, f)$ est isomorphe à $A(X)$ par f^{tr}.* ∎

Remarque 3. — Si f est définie par des polynômes P_i, f est polynomialement inversible à gauche ssi $\mathcal{F}\{P\} = A(X)$, en identifiant les P_i avec leurs images par l'injection canonique de $\mathcal{F}\{n\}$ dans $A(X)$.

On remarque qu'il est question ici d'applications polynomiales de X dans Y, et non de morphismes de variétés algébriques différentielles. Certains morphismes peuvent en effet ne pas être polynomiaux (cf. chap. I § 4 n° 4 rem. 3 p. 14).

4. Problèmes

Après ces préliminaires, nous allons définir de manière plus précise les problèmes dont nous nous proposons de donner une solution algorithmique.

PROBLÈME 1. — *Soit f une application rationnelle de X dans Y, tester si f est inversible.*

On peut transcrire ce problème de la manière suivante. Les variétés X et Y sont définies par les idéaux $\mathcal{I}$ et $\mathcal{J}$ de $k\{n\}$ et $k[m]$, l'application f par m éléments de $K(X)$ $f_1, \ldots, f_m$ définis par des fractions P/Q où P et Q sont deux éléments de $A(X)$ donnés par des représentants dans $k\{n\}$.

L'inversibilité telle que nous l'avons définie ne dépend pas de Y et l'on peut donc supposer que Y est $\mathbf{A}^m$. Le problème est alors de tester si le morphisme de $\mathbf{K}(\mathrm{Im}(f))$ dans $\mathbf{K}(X)$ associé à f est un isomorphisme. Si la variété de départ est $\mathbf{A}^n$ il s'agit de tester si $k\langle f\rangle = k\langle n\rangle$.

PROBLÈME 2. — *Soit f une application birationnelle de X dans Y, déterminer l'inverse de f.*

Supposant que f est définie comme ci-dessus, on peut demander que son inverse soit défini par un système de représentants dans $\mathbf{K}(X)$.

On peut se poser les mêmes problèmes pour des applications polynomiales susceptibles d'admettre un inverse polynomial. En extrapolant, on peut se poser les problèmes plus généraux suivants.

PROBLÈME 3. — *Soit $K = \mathrm{Fr}\mathcal{F}\{n\}/\mathcal{I}$ où $\mathcal{I}$ est premier, un corps de fractions. Étant donné $\mathcal{F}(f)$ un sous-corps de K, tester si un élément donné de K appartient à $K(f)$.*

Pour résoudre ce problème, on essaiera de déterminer une méthode qui évite de répéter un calcul lourd pour chaque candidat à tester, mais permette au contraire d'obtenir une réponse rapide à partir des résultats d'une unique étape coûteuse ; c'est le cas avec les bases standard pour tester l'appartenance à un idéal.

PROBLÈME 3′. — *Soit $A = \mathcal{F}\{n\}/\mathcal{I}$ un anneau, et $B = \mathcal{F}\{P\}$ un sous-anneau de A de type fini. Étant donné un élément Q de A, tester si Q appartient à B.*

§ 2. AUTOMORPHISMES DE $k(n)$. GROUPE DE CREMONA

Dans ce paragraphe, on considérera principalement le cas algébrique, faute de résultats dans le cas différentiel. k désignera, sauf précision explicite, un corps de caractéristique quelconque.

1. Définitions. Structure

On va indiquer quelques propriétés des automorphismes de $k(n)$, en se limitant à celles qui auront des conséquences utiles pour les applications effectives.

DÉFINITION 1. — *On appelle groupe de Cremona d'ordre n et l'on note $\mathbf{Cr}(n)$ le groupe des applications birationnelles de $\mathbf{P}_n$ dans lui-même.*

Ce groupe est manifestement isomorphe au groupe des applications birationnelles de $\mathbf{A}^n$ et anti-isomorphe au groupe des automorphismes de $k(n)$.

Il est évident que $\mathbf{Cr}(1)$ est isomorphe au groupe des applications affines. Le théorème qui suit, énoncé par Max NOETHER et prouvé par CASTELNUOVO dans le cas algébriquement clos, puis étendu par Yu. I. MANIN à un corps parfait, décrit la structure de $\mathbf{Cr}(2)$.

La structure de $\mathbf{Cr}(n)$ pour $n \geq 3$ est à ce jour encore très mal connue.

THÉORÈME 1 (M. Noether – Castelnuovo – Manin). — *Sur un corps parfait, le groupe $\mathbf{Cr}(2)$ est engendré par l'ensemble des transformations quadratiques birationnelles de la forme*

$$x \mapsto \frac{a_1 x + b_1 y + c_1}{a_2 x + b_2 y + c_2},\ y \mapsto \frac{a_3 x + b_3 y + c_3}{a_4 x + b_4 y + c_4},$$

en coordonnées affines.

PREUVE. Voir [God] ou [M]. ∎

Ce théorème ne s'étend pas sous cette forme pour $n \geq 3$.

Nous allons introduire une nouvelle classe de générateurs qui nous permettra de reformuler le théorème 1.

DÉFINITION 2. — *On appelle transformation de de Jonquières une transformation birationnelle de $\mathbf{P}_n$ s'exprimant en coordonnées affines sous la forme*

$$(x_1, \ldots, x_n) \mapsto \big(x_1, \ldots, x_{n-1}, f_1(x_1, \ldots, x_{n-1})x_n + f_2(x_1, \ldots, x_{n-1})\big)$$

où $(f_1, f_2) \in k(n-1)^* \times k(n-1)$.

DÉFINITION 3. — *On appelle permutation une transformation birationnelle de $\mathbf{P}_n$ qui s'exprime dans un système de coordonnées affines sous la forme*

$$(x_1, \ldots, x_n) \mapsto (x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$

où $\sigma \in S_n$.

THÉORÈME 2. — *Le groupe $\mathbf{Cr}(2)$ est engendré par les permutations et les transformations de de Jonquières.* ∎

On ignore si sous cette forme le théorème s'étend ou non au cas $n \geq 3$. Ritt signalait en 1950 dans [Ri2] comme problème ouvert l'existence éventuelle d'un analogue du résultat de Noether en algèbre différentielle. À ma connaissance, aucune avancée n'a été faite dans ce sens depuis lors.

2. Degré de l'inverse d'une transformation birationnelle

Le théorème qui suit présentera un intérêt majeur pour borner la complexité de nombreux algorithmes. Son origine exacte est incertaine et il était peut-être, de longue date, "bien connu" quoique non publié. Une démonstration, due à O. GABBER, en est donnée dans [BCW].

THÉORÈME 3. — *Si f est une transformation birationnelle de $\mathbf{P}_n$,*

$$\deg f^{-1} \leq (\deg f)^{n-1}.$$

PREUVE. Voir [BCW]. ∎

Remarque 1. — Cette borne est fine. En effet, l'inverse de la transformation de degré d, définie en coordonnées affines par

$$(x_1, \ldots, x_n) \mapsto (x_1, x2 + x_1^d, \ldots, x_n + x_{n-1}^d),$$

est de degré d^{n-1}.

La notion de degré d'une transformation rationnelle s'exprime le plus naturellement en coordonnées projectives. Or nous devrons dans les applications travailler dans un repère affine où une définition différente, bien que non intrinsèque, est plus immédiate et mieux adaptée.

DÉFINITION 4. — *Soit f une transformation rationnelle de $\mathbf{A}^n$, Rep un repère affine, on appelle degré affine de f dans le repère Rep (et l'on note* $\deg_{\mathrm{aff}}(f, Rep)$ *le degré maximal des numérateurs et dénominateurs des fractions définissant f dans ce repère.*

Remarques. — 2) Contrairement au degré qui s'étend sans ambiguïté du cas projectif au cas affine, le degré affine dépend du plongement de $\mathbf{A}^n$ dans $\mathbf{P}_n$ ainsi que du système de coordonnées affines choisi.

3) Néanmoins, si f est polynomiale, le degré projectif et le degré affine de f coïncident.

4) Le degré projectif majore le degré affine. Mais on a seulement $\deg f \leq (\deg_{\mathrm{aff}})^n$.

Souhaitant disposer d'un analogue du théorème précédent dans le cas affine, on peut utiliser le corollaire suivant.

COROLLAIRE 1. — *Soit f une transformation birationnelle de $\mathbf{A}^n$, pour tout couple de repères affines Rep_1 et Rep_2, on a*

$$\deg_{\mathrm{aff}}(f^{-1}, Rep_1) \leq \deg_{\mathrm{aff}}(f, Rep_2)^{n(n-1)}.$$

PREUVE. Il suffit d'appliquer le théorème en utilisant la remarque 4. ∎

En fait, la borne donnée par le corollaire est trop large. Le théorème qui suit montre qu'on dispose pour le degré affine d'une borne plus proche de celle sur le degré projectif.

THÉORÈME 4. — *Soit f une transformation birationnelle de $\mathbf{A}^n$, définie dans un repère par n fractions f_i/g_i, alors*

$$\deg(f^{-1}) \leq \prod_{i=1}^{n} \max(\deg f_i, \deg g_i + 1).$$

PREUVE. On peut trouver deux ouverts de Zariski U et V définis respectivement par $R \neq 0$ et $S \neq 0$, denses dans $\mathbf{A}^n$, tels que f définisse une bijection entre U et V. Soit $H_0 = V(P_0)$ un hyperplan de $\mathbf{A}^n$ tel que $H_0 \notin V(S)$. Soit d le degré de la variété $f(H_0)$. d est égal au degré (projectif!) de f^{-1}. On peut trouver $n-1$ hyperplans $H_1, \ldots, H_{n-1}$, définis par des formes linéaires L_i, tels que $V_0 \cap H_1 \cap \ldots \cap H_{n-1}$ soit constitué de d points distincts de U'.

Soit p un de ces points, on lui associe le point de $\mathbf{A}^n \times \mathbf{A}^n$ $(f^{-1}(p), p)$, de coordonnées $(x_1, \ldots, x_n, y_1, \ldots, y_n)$. (x, y) est solution du système

$$\begin{aligned} L_i(y) &= 0 \quad i = 1, \ldots, n \\ f_j(x) - g_j(x) y_j &= 0 \quad j = 1, \ldots, n, \end{aligned}$$

où les f_i/g_i sont les fractions définissant f.

Réciproquement, à tout point solution de ce système, qui n'est pas dans $U \times V$, correspond un point de $V_0 \cap H_1 \cap \ldots \cap H_{n-1}$. Les n premiers polynômes sont linéaires, tandis que le degré du $n + i^{\text{ème}}$ est $\max(\deg f_i, \deg g_i + 1)$. Appliquant le théorème de Bézout, il suffit de remarquer que d est égal à $\deg(f^{-1})$ pour conclure. ■

COROLLAIRE 1. — *Sous les hypothèses du théorème,*

$$\deg_{\text{aff}}(f^{-1}, Rep_1) \leq \left(deg_{aff}(f, Rep_2) + 1\right)^n.$$

PREUVE. C'est une conséquence immédiate du théorème en remarquant que

$$\max(\deg f_i, \deg g_i + 1) \leq \deg_{\text{aff}} f + 1,$$

et que le degré projectif majore le degré affine. ■

Remarques. — 5) La borne du théorème peut être atteinte. Il suffit de considérer l'application définie par $(x_1, \ldots, x_n) \mapsto (x_1, x_2 + x_1^{e_1}, \ldots, x_n + x_{n-1}^{e_{n-1}})$. Le degré de l'inverse est $\prod_{i=1}^{n-1} e_i$. On peut noter que dans ce cas la majoration est meilleure qu'avec le théorème de Gabber.

6) En revanche, la majoration donnée par le corollaire n'est pas optimale. Kossivi ADJAMAGBO et Pierre BOURY ont récemment prouvé l'égalité $\deg_{\text{aff}}(f^{-1}) = \deg_{\text{aff}}(f)$, dans le cas rationnel à deux variables, par des méthodes donnant une expression de l'inverse grâce à des calculs de résultants (cf. [AB]).

3. Ordre de l'inverse d'une application birationnelle différentielle

On retourne au cas différentiel pour donner un analogue différentiel du théorème précédent dans le cas d'une transformation birationnelle de $\mathbf{A}^n$. La preuve de Gabber utilise le théorème de Bézout. On va lui substituer l'analogue différentiel du théorème de Bézout donné au chapitre I. À ceci près, en dépit de quelques complications techniques propres au cas différentiel, la preuve suit de très près celle donnée par Gabber, dont s'inspire aussi la version affine ci-dessus.

THÉORÈME 5. — *Soit f une transformation birationnelle de $\mathbf{A}^n$, l'ordre de f^{-1} est inférieur ou égal à $n \operatorname{ord} f$. Plus précisément, si les fractions f_i définissant f ont un ordre maximal e_i en la variable x_i,* $\operatorname{ord} f^{-1} \leq e_1 + \cdots + e_n$.

PREUVE. On note m le cardinal de l'ensemble de dérivations de $\mathcal{F}$.

On choisit dans $\mathbf{A}^n$ des hyperplans génériques $H_0, H_1, \ldots, H_{n-1}$, c'est-à-dire des hyperplans définis par des polynômes linéaires $L_i = (\sum_{i=1}^n \epsilon_{i,j} x_j) + \epsilon_{i,0}$, où les $\epsilon_{i,j}$ sont génériques sur $\mathcal{F}$. La variété $f\,H_0$ est une hypersurface irréductible, qui est la composante générale d'un polynôme P d'ordre $\operatorname{ord} f^{-1}$. En effet, si f^{-1} est définie par les fractions R_i/Q_i, on obtient P en divisant le numérateur de $L_0(R/S)$, considéré comme un polynôme en les $\epsilon_{i,j}$, par son contenu dans $\mathcal{F}\{n\}$.

On note $\mathcal{G}$ l'extension $\mathcal{F}\langle\epsilon\rangle$. f s'étend naturellement en une application birationnelle sur $\mathbf{A}^n_{\mathcal{G}}$. En utilisant la proposition I.4.3.10 p. 19, $f\,H_0 \cap \bigcap_{i=1}^{n-1} H_i$ est une variété irréductible de $\mathbf{A}^n_{\mathcal{G}}$ de type différentiel $m-1$ et d'ordre $\operatorname{ord} f^{-1}$. On choisit un zéro générique η de cette variété.

L'extension $\mathcal{G}\langle f^{-1}\,\eta\rangle$ est $\mathcal{G}$-isomorphe à $\mathcal{G}\langle\eta\rangle$. D'après la proposition I.4.2.8 p. 19, il existe un entier h tel que $\omega_{\eta/\mathcal{G}}(r-h) \leq \omega_{f^{-1}\,\eta/\mathcal{G}}(r) \leq \omega_{\eta/\mathcal{G}}(r+h)$. Les deux extensions ont donc le même type différentiel $m-1$ et le même ordre.

Utilisant l'équivalence birationnelle, $f^{-1}\,\eta$ est un point générique de la variété irréductible $V = H_0 \cap \bigcap_{i=1}^{n-1} f^{-1} H_i$. L'ensemble de polynômes

$$\Sigma = \{L_0, \operatorname{denom} L_i(P/Q)\ 1 \leq i \leq n-1\},$$

où P_i/Q_i est la fraction réduite correspondant à f_i, est tel que l'idéal $[\Sigma] : [\prod_{i=1}^n Q_i]^\infty$ définisse V. Cet idéal est donc une composante de $\{\Sigma\}$. Appliquant le théorème I.4.3.2 p. 21, on conclut que l'ordre de V est inférieur ou égal à $e_1 + \cdots + e_n$, puisque chacun des polynôme de Σ a un ordre en x_i borné par e_i. Ceci majore donc également l'ordre de f^{-1}. ∎

Remarques. — 1) Sous la forme de la deuxième assertion du théorème, la borne est fine. Il suffit en effet de considérer l'application définie par $(x_1, \ldots, x_n) \mapsto (x_1, x_2 + x_{1,(e_1)}, \ldots, x_n + x_{n-1,(e_{n-1})})$, dont l'inverse est exactement d'ordre $e_1 + \cdots + e_{n-1}$. L'analogie avec le cas algébrique laisserait attendre une borne de la forme $(n-1)\operatorname{ord} f$. J'ignore s'il existe un contre-exemple.

2) Dans le cas d'une application d'ordre nul, on retrouve le résultat de la remarque 1.3.2. p. 25.

§ 3. AUTOMORPHISMES DE $k\{n\}$ ET $\mathbf{A}^n$

1. Structure

Le problème de la structure du groupe des automorphismes de $\mathbf{A}^n$, est très similaire à celui des automorphismes du groupe de Cremona. Là encore, on connaît peu de choses pour $n \geq 3$. Pour $n = 1$ il s'agit du groupe linéaire, pour $n = 2$ on dispose du théorème suivant, analogue au théorème de Noether, qui fut démontré pour la première fois par H.W.E. JUNG en 1942 (cf. [J]) dans le cas d'un corps de caractéristique nulle, et dans le cas général par W. VAN DER KULK en 1953 (cf. [Ku]).

THÉORÈME 1 (Jung–van der Kulk). — *Le groupe des automorphismes de $\mathbf{A}^2$ est engendré par les applications des deux types suivants :*

$$(*) \qquad (x, y) \mapsto (y, x)$$

$$(**) \qquad (x, y) \mapsto (x, ay + P(y)) \quad a \neq 0.$$

PREUVE. Cf [Ku]. ■

Ce groupe est donc engendré par l'involution permutant les variables et les applications de de Jonquières polynomiales. On peut le voir, en caratéristique 0, comme la conséquence du théorème qui va suivre. Il a été énoncé pour la première fois en 1956, dans le cas complexe, par SEGRE (cf. [Se]), qui en a donné une démonstration erronée. La première démonstration complète est due à S.S. ABHYANKAR et T.-T. MOH en 1975.

THÉORÈME 2 (Segre, Abhyankar–Moh). — *Soient k un corps de caractéristique 0, P et Q deux polynômes en une variable x sur k. Alors, si $k[P, Q]$ est égal à $k[x]$ et si le degré de P est inférieur ou égal à celui de Q, $\deg P$ divise $\deg Q$.*

PREUVE. Voir [AM]. ■

De ces théorèmes découlent des méthodes particulièrement simples et efficaces pour tester que $k[P, Q]$ est égal à $k[x, y]$ ou $k[x]$ en utilisant une version légèrement modifiée de l'algorithme de base canonique (cf. chap. III § 3 n° 6).

2. Caractérisation. Conjecture jacobienne

Soit f une application polynomiale de $\mathbf{A}^n$ dans $\mathbf{A}^n$ définie par n polynômes f_i. Notons $J(f)$ la matrice $(\partial f_i/\partial x_i)$. Si f admet un inverse polynomial f^{-1}, on doit avoir $J(f^{-1})J(f) = \mathrm{Id}$ et donc $J(f) \in k$. La conjecture jacobienne propose une réciproque.

CONJECTURE — *Soit f une application polynomiale sur un corps k de caractéristique 0, alors*

$$\det\ J(f) \in k \Rightarrow f \textit{polynomialement inversible.}$$

Remarque 1. — Une conjecture analogue en caractéristique p positive est fausse. Il suffit de considérer en une variable $x \mapsto x^p + x$.

Cette conjecture, formulée par O. H. KELLER en 1939, reste depuis lors un problème ouvert, même en deux variables. Elle a néanmoins été prouvée par MOH en deux variables pour $\deg f \leq 100$. D'autre part, S. WANG a démontré qu'elle est vraie quel que soit le nombre de variables, si $\deg f \leq 2$. Ce résultat s'avère également en caractéristique $p \geq 3$.

La conjecture jacobienne ne jouera pas en elle-même un rôle essentiel dans notre approche, bien qu'elle puisse fournir, si elle est démontrée, un test effectif d'existence de l'inverse. Cependant, de nombreux résultats qui nous seront fort utiles, comme la borne de GABBER, proviennent de travaux qui lui sont liés. Le théorème 2 été énoncé dans un article où Segre donnait une démonstration erronée de cette conjecture difficile et dangereuse : W. Groebner, et d'autres en ont donné des “démonstrations”.

On pourra trouver de plus amples détails sur l'histoire et l'état des recherches à ce sujet, dans l'article de H. BASS *et al.* [BCW]. Nous allons donner un théorème qui résume quelques-unes des propriétés connues caractérisant les automorphismes de $\mathbf{A}^n$.

THÉORÈME 3. — *Soit f une transformation polynomiale de $\mathbf{A}^n_k$, où k désigne un corps quelconque. Les énoncés suivants sont équivalents.*

a) f est un automorphisme.

b) $J(f) \in k$ et $k(f) = k(n)$.

c) $J(f) \in k$ et l'application de k^n dans lui-même induite par f est injective.

PREUVE. Voir [BCW]. ∎

On a également la propriété suivante, qui complète le dernier énoncé.

PROPOSITION 1. — *Si une application polynomiale f est injective sur k^n, où k est algébriquement clos, alors f admet un inverse polynomial.*

PREUVE. Ceci signifie que $(x_i - y_i)^p \in [P_j(x) - P_j(y)\ 1 \leq j \leq n]$. Donc, en anticipant sur la suite et en utilisant le corollaire de la proposition 4.2.5 p. 36, f admet un inverse rationnel. Supposons que cet inverse ne soit pas polynomial. Il est défini par des fractions réduites R_i/S_i avec $S_i \neq 1$ pour un certain indice i. L'ensemble des points tels que $S_i(P) = 0$ est non vide puisque k est algébriquement clos et a toutes ses composantes de dimension $n - 1$. Or son image est incluse dans l'ensemble des 0 de R_i et S_i qui a des composantes de dimension au plus $n - 2$. Ceci contredit l'injectivité. ∎

Cette démonstration ne peut pas s'étendre au cas différentiel. En effet, même si P et Q sont premiers entre eux, il se peut que $V(P, Q)$ soit de dimension $n - 1$: prendre $P = \delta^2 x$ et $P = \delta x$. J'ignore en revanche si la proposition elle-même reste vraie, ou s'il existe un contre-exemple.

§ 4. IDÉAUX ASSOCIÉS À UNE APPLICATION RATIONNELLE

Dans ce paragraphe, on considère une application rationnelle affine $f \colon X \subset \mathbf{A}^n_{\mathcal{F}} \mapsto \mathbf{A}^m_{\mathcal{F}}$, définie par m fractions de $\mathbf{K}(X)$, supposées données par des représentants P_i/Q_i dans $\mathrm{Fr}\mathcal{F}\{x_1, \ldots, x_n\}/\mathcal{I}(X)$.

1. Graphe

Suivant une méthode classique, on peut ramener l'étude d'une application rationnelle à celle de son graphe. Le graphe peut être défini ensemblistement en considérant le graphe de la fonction associée. Mais en ce sens, le graphe n'est pas un ensemble algébrique. On considère donc l'adhérence de Zariski du graphe ensembliste, qui n'est plus un graphe, mais définit néanmoins de manière unique une application rationnelle. En fait, on s'intéressera surtout l'idéal associé.

DÉFINITION 1. — *Soit f une application rationnelle de graphe ensembliste G dans $\mathbf{A}^n \times \mathbf{A}^m$, on appelle idéal graphe de f (ou graphe lorsqu'il n'y a pas de risque de confusion) et l'on note $\Gamma(f)$ l'idéal $\mathcal{I}(G)$.*

Lemme 1. — *Si η est un point générique de X, $f(\eta)$ est un point générique de* $\mathrm{Im}(f)$ *et $(\eta, f(\eta))$ un point générique de $\Gamma(f)$.*

PREUVE. f est continue sur l'ouvert $\mathrm{Dom}\, f$, et η dense dans cet ouvert. Par continuité, $f(\eta)$ est dense dans $f\,\mathrm{Dom}\, f$ et donc dense dans $\mathrm{Im}\, f$. On raisonne de manière identique pour le graphe, en considérant l'application $\mathrm{Id} \times f \colon X \times \mathrm{Im}\, f$. ∎

Ceci implique en particulier que le graphe est premier, que $\Gamma f \cap \mathcal{F}\{x_1, \ldots, x_n\} = \mathcal{I}(X)$ et que $\Gamma f \cap \mathcal{F}\{y_1, \ldots, y_m\} = \mathcal{I}(\mathrm{Im}\, f)$.

PROPOSITION 1. — *Un idéal $\mathcal{I}$ de $\mathcal{F}\{x_1, \ldots, x_n, y_1, \ldots, y_m\}$ est le graphe d'une application rationnelle f de $X \subset \mathbf{A}^n$ dans A^m ssi les trois conditions suivantes sont satisfaites :*

i) $\mathcal{I}$ est premier,

ii) $\forall i = 1, \ldots, m\ \exists P_i \in \mathcal{F}\{n\}\ \exists Q_i \notin \mathcal{I}(X)\quad P_i(x) - Q_i(x) y_i \ \in\ \mathcal{I}$,

iii) $\mathcal{I} \cap \mathcal{F}\{x_1, \ldots, x_n\} = \mathcal{I}(X)$.

Dans cette situation, les m fractions P_i/Q_i définissent l'application correspondante.

PREUVE. L'implication directe est immédiate. Vérifions la réciproque. Soit f l'application définie par les fractions P/Q. On va montrer que $\mathcal{I}$ est le graphe de f. Soit η un point générique de X, la condition iii) implique qu'on puisse trouver η' tel que (η, η') soit un zéro générique de $\mathcal{I}$. Mais alors, ii) implique que η' est égal à $f(\eta)$. Comme $\mathcal{I}$ est premier, d'après i), c'est l'idéal définissant l'adhérence de $(\eta, f(\eta))$, donc le graphe de f. ∎

COROLLAIRE 1. — $\Gamma f = \mathcal{J} := [\mathcal{I}(X), P_i(x) - Q_i(x) y_i \ i \in [1, m]] : (\prod_{i=1}^m Q_i(x))^\infty$.

PREUVE. Les conditions ii) et iii) sont immédiatement satisfaites. Reste à s'assurer que l'idéal $\mathcal{J}$ est premier. Maintenant, un polynôme R appartient à $\mathcal{J}$ ssi

$$\left(\prod_i^m Q_i^{\deg_{y_i} R}\right) R(x, f(x)) \in \mathcal{I}(X).$$

Comme $\mathcal{I}(X)$ est premier, on en déduit immédiatement que si $RS \in \mathcal{J}$

$$\left(\prod_i^m Q_i^{\deg_{y_i} R}\right) R(x, f(x)) \ \left(\prod_i^m Q_i^{\deg_{y_i} S}\right) S(x, f(x)) \in \mathcal{I}(X),$$

donc que R ou S appartiennet à $\mathcal{J}$. La conclusion est alors claire d'après la propriété. ∎

Corollaire 2. — *Si f est inversible, le graphe de f^{-1} restreinte à* $\mathrm{Im}(f)$ *est*

$$\{P(y_1, \ldots, y_n, x_1, \ldots, x_m) | P \in \Gamma(f)\}.$$

■

Remarque 1. — Selon une technique classique, le graphe de f est égal à l'idéal

$$\left[\mathcal{I}(X), P_i(x) - Q_i(x)y_i \ i \in [1, m], u\left(\prod_{i=1}^{m} Q_i(x)\right) - 1\right]_{\mathcal{F}\{x,y,u\}} \cap \mathcal{F}\{x, y\}.$$

On pourrait aussi choisir autant de variables u qu'il y a de dénominateurs non nuls, ou remplacer le produit par le pgcd des Q_i.

Corollaire 3. — *Soit f une application rationnelle, $\mathcal{J}$ l'idéal de $\mathcal{F}\{m\}$ définissant* $\mathrm{Im}(f)$*, alors f est inversible ssi*

$$\forall i \in 1, \ldots, n \, \exists P_i \in \mathcal{F}\{m\} \, \exists Q_i \in \mathcal{F}\{m\} \setminus \mathcal{J} \quad P_i(y) - Q_i(y)x_i \in \Gamma(f).$$

Si c'est le cas, les fractions P_i/Q_i définissent l'inverse. ■

Il n'est bien sûr pas utile de construire le graphe lui-même, ce qui nécessiterait en pratique de faire une élimination. On peut conclure directement en considérant l'idéal de $\mathcal{F}\{x, y, u\}$, défini par la remarque précédente.

Le graphe nous permet donc de ramener l'étude de l'inversibilité d'une application rationnelle à la recherche d'éléments d'un type particulier dans un idéal. Nous verrons que ceci peut être fait de manière effective en utilisant des méthodes désormais classiques de résolution d'un système d'équations polynomiales telle que les algorithmes de bases standard ou la méthode de Ritt–Wu.

On dispose d'une technique permettant de traduire les propriétés des applications rationnelles — et donc des sous-corps engendrés par les fractions qui les définissent — à l'aide d'idéaux associés. On peut la raffiner à loisir.

Lemme 2. — *Un élément g de $K(X)$ appartient à $\mathcal{F}\langle f\rangle$ (resp. $\mathcal{F}\{f\}$) ssi on a le diagramme*

$$\begin{array}{ccc} X & \longrightarrow & f(X) \\ & \searrow g & \downarrow h \\ & & \mathbf{A}^1, \end{array}$$

où h désigne une application rationnelle (resp. polynomiale). ■

Lemme 3. — *Soient $f : X \mapsto Y$ et $g : Y \mapsto Z$ deux applications rationnelles avec f dominante, le graphe de $g \circ f$ est l'idéal*

$$[\Gamma(f), \Gamma(g)]_{\mathcal{F}\{x,y,z\}} \cap \mathcal{F}\{x, z\}.$$

■

Ces deux lemmes immédiats impliquent le résultat suivant.

PROPOSITION 2. — *Pour toute famille finie f de fractions de K, et tout élément $g = R/S$ de K, g appartient à $\mathcal{F}(f)$ (resp. $\mathcal{F}\{f\}$) ssi l'idéal*

$$[\Gamma\, f, R(x) - zS(x)]_{\mathcal{F}\{x,y,z\}}$$

contient un élément de la forme $T(y) - zU(y)$ (resp $z - T(y)$). ∎

SHANNON et SWEEDLER on beaucoup utilisé cette idée — qu'ils attribuent à SPEAR — avec des techniques de bases standard dans le cas d'applications rationnelles sur $\mathbf{A}^n$. Ils l'appellent méthode des variables marquées (*tag variables*), du nom qu'ils donnent aux variables y_i dans les polynômes définissant le graphe.

2. Idéal Δ associé à un sous-corps

On introduit ici une méthode différente, qui permet en toute généralité de ramener le problème d'appartenance d'une fraction à un sous-corps de $\mathbf{K}(X)$, à l'appartenance d'un polynôme à un idéal, ne dépendant intrinsèquement que du sous-corps, et non des générateurs choisis, comme c'est le cas pour le graphe. On identifie $\mathbf{K}(X)$ avec $\mathrm{Fr}\mathcal{F}\{xnyn\}/\mathcal{I}(X)$.

DÉFINITION 2. — *Soit K un sous-corps de $\mathbf{K}(X)$, on appelle idéal Δ de K et l'on note $\Delta_{\mathcal{F}}(K)$ l'idéal de $K\{n\}$ défini par*

$$\Delta(K) = \left[P(x) - Q(x)\frac{P(y)}{Q(y)} \;\middle|\; P/Q \in K \right]_{K\{x_1,\ldots,x_n\}}.$$

Par la suite, on notera seulement $\Delta(K)$, lorsqu'il n'y aura pas ambiguïté.

PROPOSITION 3. — *Pour tout sous-corps K de $K(X)$, $\Delta(K) = \{P \in K\{n\} | P(y) = 0\}$. Cet idéal est premier.*

PREUVE. L'inclusion de gauche à droite est immédiate. Réciproquement, si $P(y) = 0$, P est égal à $P(x) - P(y)$ qui est dans $\Delta(K)$.

Montrons que l'idéal est premier. Si PQ est dans l'idéal, $(PQ)(y) = 0$. On en déduit que $P(y)$ ou $Q(y)$ doivent être nuls et donc que P ou Q sont dans l'idéal. ∎

De la seconde expression de l'idéal, on déduit facilement le résultat suivant.

COROLLAIRE 1. — *$\Delta(K) \cap \mathcal{F}\{x_1, \ldots, x_n\}$ est égal à $\mathcal{I}(X)$.* ∎

PROPOSITION 4. — *Si $K = \mathcal{F}(f)$ où $f_i = P_i/Q_i$ $i \in [1, m]$, posons*

$$\mathcal{J} = \left[P_i(x) - Q_i(x)\frac{P_i(y)}{Q_i(y)}; u\left(\prod_{i=1}^{m} Q_i(x)\right) - 1 \right]_{K\{x_1,\ldots,x_n,u\}}.$$

Alors, $\Delta(K) = \mathcal{J} \cap K\{x_1, \ldots, x_n\}$.

PREUVE. D'après le corollaire, les polynômes Q_i n'appartiennent pas à $\Delta(K)$. Ceci assure l'inclusion de droite à gauche.

$\Delta(K)$ est engendré par les polynômes de la forme $A = R(x) - (R(y)/S(y))S(x)$ $R/S \in K$. Comme les fractions P_i/Q_i engendrent K, on voit que A multiplié par un produit de puissances des Q_i appartient à l'idéal $[P_i(x) - Q_i(x)P_i(y)/Q_i(y)\ i \in [1, m]]$, et donc que A est dans $\mathcal{J}$. ∎

PROPOSITION 5. — *Une fraction P/Q de $K(X)$ est dans K ssi*

$$P(x) - Q(x)\frac{P(y)}{Q(y)} \in \ [\Delta(K)]_{\mathbf{K}(X)\{n\}} = \mathbf{K}(X)\Delta(K)$$

PREUVE. C'est manifestement une condition nécessaire. Supposons là satisfaite. On peut se donner une base $(e_i)i \in I$ de $\mathbf{K}(X)$ sur K, avec $e_{i_0} = 1$. Décomposant $P(y)/Q(y)$ dans cette base, on trouve $P(y)/Q(y) = c_{i_0} + \sum_{i \in I \setminus \{i_0\}} c_i e_i$. Alors, $P(x) - c_{i_0}Q(x) \in \Delta(K)$, ce qui implique que $P(y)/Q(y) = e_{i_0} \in K$, en utilisant la proposition 4. ■

On en déduit immédiatement le corollaire.

COROLLAIRE 1. — *Une application rationnelle f sur X est inversible ssi $(x_i - y_i) \in \Delta(\mathcal{F}(f))$ $i \in [1, n]$.* ■

On voit que la construction de l'idéal Δ permet de tester l'appartenance d'un élément à un sous-corps et l'existence d'un inverse pour une application rationnelle, dès lors que l'on sait tester l'existence d'un élément à un idéal. Or ceci peut être fait en utilisant un algorithme de bases standard dans le cas algébrique, et sous certaines réserves dans le cas différentiel (voir chap. IV § 1).

On verra aussi qu'on peut utiliser une version adaptée des algorithmes de RITT–WU, voisine de celle de Daniel LAZARD (cf. [La]). Le fait que $\Delta(K)$ est premier, et qu'on dispose d'un test effectif d'appartenance par la prop. 3 p. 35, jouant alors un rôle crucial pour construire un *véritable* ensemble caractéristique (3), au sens de la déf. I.4.1.9 p. 16. Cette méthode est détaillée au chap. IV § 2.

Bien que fort naturelle, cette méthode semble moins connue que celle utilisant le graphe. Elle a été utilisée par RITT à titre d'argument, dans sa démonstration d'un analogue du théorème de Lüroth sur un corps différentiel simple (voir [Ri2 chap. II n° 41]). Je n'en connais pas d'application explicite au calcul formel antérieure à mes travaux, mais elle est implicitement contenue dans la méthode utilisée par LECOURTIER et RAKSANYI pour tester l'identifiabilité structurelle globale. Leur méthode de résolution est très proche de celle de Ritt–Wu, mais ils n'ont pas tiré parti du fait que l'idéal peut être considéré comme premier.

Remarque 1. — Il existe une relation entre le graphe d'une application rationnelle et l'idéal Δ associé. En effet, on peut considérer y comme un point générique de X et donc $f\,y$ comme un point générique de l'image. L'idéal Δ s'interprète alors naturellement comme une section générique du graphe.

§ 5. IDÉAUX ASSOCIÉS À UNE SOUS-ALGÈBRE

Dans ce paragraphe, on notera f une application rationnelle de $X \subset \mathbf{A}^n$ dans $X \subset \mathbf{A}^m$, définie par m polynômes f_i. Identifiant les f_i avec les éléments de $\mathcal{F}\{n\}/\mathcal{I}(X)$ correspondant, on appellera A l'anneau $\mathcal{F}\{f\}$.

(3) On a besoin de cette construction, car la prop. 3 ne s'applique pas pour un polynôme de $\mathbf{K}(X)\{n\}$!

1. Graphe

La situation est identique à celle du § 4, mais on souhaite maintenant caratériser à l'aide du graphe qu'une application rationnelle admet un inverse polynomial, ou plus généralement qu'une fraction rationnelle donnée appartient à la sous-algèbre A. Une réponse théorique est fournie par le théorème suivant. On verra en III.2.1 qu'on peut en déduire des tests algorithmiques.

THÉORÈME 1. — *Soit $g = P/Q$ une fraction de $\mathbf{K}(X)$, alors $g \in A$ ssi il existe $R \in \mathcal{F}\{m\}$ tel que $P(x) - Q(x)R(y) \in \Gamma(f)$ et alors $g = R(f)$.*

PREUVE. $\Longrightarrow$ est immédiat.

$\Longleftarrow$ Si l'on a $P(x) - Q(x)R(y) \in \Gamma(f)$, alors $P(x) - Q(x)R(f(x)) = 0$ et comme $Q(x) \neq 0$, on a bien $P(x)/Q(x) = R(f)$. Ceci achève la démonstration. ∎

COROLLAIRE 1. — *f admet une réciproque polynomiale ssi pour tout $i \in [1, n]$ il existe $R_i \in \mathcal{F}\{m\}$ tel que $x_i - R_i(y) \in \Gamma(f)$ et alors f^{-1} est définie par les polynômes R_i.* ∎

2. Idéal Σ

On pourrait généraliser la construction de l'idéal Δ, mais cela ne semble pas déboucher sur une méthode effective intéressante. On opte donc pour une construction légèrement différente, mais qui conduit aussi à un idéal ne dépendant que de $\mathcal{F}\{f\}$. Elle ne débouche sur un test effectif d'appartenance à une sous-algèbre que sous certaines hypothèses, mais s'applique en contrepartie à certaines algèbres non finiment engendrée. Pour simplifier, on se restreindra à des applications $f : \mathbf{A}^n \mapsto \mathbf{A}^n$, et à des sous-algèbres de $\mathcal{F}\{n\}$.

DÉFINITION 1. — *Soit E une sous-ensemble de $\mathcal{F}\{n\}$, on appelle idéal Σ associé à E et l'on note $\Sigma_{\mathcal{F}}(E)$ l'idéal*

$$[P(x) - P(y) | P \in E]_{\mathcal{F}\{x_1,\ldots,x_n,y_1,\ldots,y_n\}}.$$

Par la suite, on notera simplement $\Sigma(E)$, s'il n'y a pas ambiguïté.

Lemme 1. — *Soit B l'ensemble des polynômes P de $\mathcal{F}\{n\}$ tels que $P(x) - P(y) \in \Sigma(E)$. B est une sous-algèbre différentielle de $\mathcal{F}\{n\}$ et l'on a $\mathcal{F}\{E\} \subset B \subset \mathcal{F}\langle A\rangle$.*

PREUVE. Pour s'assurer que c'est bien une sous-algèbre, il suffit de vérifier que si $P(x) - P(y)$ et $Q(x) - Q(y)$ sont dans $\Sigma(A)$, alors $(P+Q)(x) - (P+Q)(y)$ est dans $\Sigma(A)$ de même que $(PQ)(x) - (PQ)(y)$ et $\alpha P(x) - \alpha P(y)$ pour toute constante α. Cette sous-algèbre est stable par dérivation, car $P(x) - P(y) \in \Sigma(A)$ implique $\delta_i P(x) - \delta_i P(y) \in \Sigma(A)$.

La première inclusion est immédiate. D'autre part, si $P(x) - P(y) \in \Sigma(E)$, $P(x) - P(y) \in \Delta(\mathcal{F}\langle E\rangle)$, et donc d'après la prop. 4.2.5 p. 36, $P \in \mathcal{F}\langle E\rangle$. ∎

DÉFINITION 2. — *On appelle idéal Σ associé à une application polynomiale f, et l'on note $\Sigma(f)$ l'idéal $\Sigma(\mathcal{F}\{f\}$.*

PROPOSITION 1. — *Si $A = \mathcal{F}\{P_1, \ldots, P_m\}$ est une sous-algèbre de $\mathcal{F}\{n\}$ telle que $\mathcal{F}\langle A\rangle \cap \mathcal{F}\{n\} = A$, alors P est un élément de A ssi $P(x) - P(y)$ est dans $\Sigma(A)$.*

PREUVE. C'est une conséquence immédiate du lemme. ∎

Les informations fournies par l'étude de cet idéal sont moins précises, mais elle peuvent donner des indications utiles et permettre de traiter certains cas particuliers.

PROPOSITION 2. — *Si f est une application polynomiale, on a les trois énoncés suivant.*

a) Si f est polynomialement inversible, alors $\Sigma(f) = [x_i - y_i]$.

b) Si $\Sigma(f) = [x_i - y_i]$, alors f est rationnellement inversible.

c) L'application f est injective ssi pour tout x_i il existe $p \in \mathbf{N}$ tel que $(x_i - y_i)^p \in \Sigma(f)$.

PREUVE. a) et c) sont immédiats (4). Pour b), il suffit de remarquer que cela implique que $\Delta(f) = [x_i - y_i]$. ■

COROLLAIRE 1. — *Une application polynomiale d'ordre 0 $f \colon \mathbf{A}^n \mapsto \mathbf{A}^n$ admet un inverse polynomial ssi $\Sigma(f) = [x_i - y_i]$.*

PREUVE. D'après la proposition, c'est une condition suffisante. Comme f est d'ordre 0, on se ramène à considérer l'application rationnelle algébrique g associée. Cela implique que g est injective sur la clôture algébrique de $\mathcal{F}$,et l'on utilise la prop. 3.2.1 p. 32. ■

On retrouvera cette méthode dans le cas algébrique au chap. III § 2 n° 2, pour des applications effectives reposant sur des calculs de bases standard.

(4) Notons que f est définie sur $\mathbf{A}^n = \mathcal{U}^n$, où $\mathcal{U}$ désigne une extension universelle de $\mathcal{F}$, qui est en particulier algébriquement close.

SECONDE PARTIE

Méthodes effectives

CHAPITRE III

Bases standard. Bases canoniques

Si E est un espace vectoriel, on notera $E_\star$ l'ensemble $E \setminus \{0\}$. Si $e_1, \ldots, e_i$ sont des éléments d'un espace vectoriel E, on notera $(e_1, \ldots, e_i)$ le sous-espace vectoriel engendré par $e_1, \ldots, e_i$.

§ 1. UN CADRE GÉNÉRAL POUR LA RÉÉCRITURE ALGÉBRIQUE

1. Le cadre

Nous allons présenter un cadre général permettant de décrire tant les bases standard d'idéaux algébriques que les bases canoniques de sous-algèbres et les bases standard d'idéaux différentiels. Nous nous limiterons toutefois à considérer des objets ayant une structure d'espace vectoriel sur un corps k quelconque, mais il s'agit surtout de montrer que les bases standard d'idéaux, les bases canoniques et les bases standard d'idéaux différentiels qui seront introduites par la suite relèvent bien d'un même cadre théorique. À ce titre, la lecture de ce paragraphe n'est pas indispensable pour la suite, où les définitions nécessaires seront reprises dans chaque cas particulier.

On considérera donc une structure $\mathcal{A}$, incluant la structure d'espace vectoriel sur un corps k, et le fait que pour tout domaine D muni de cette structure D est muni d'une structure $\mathcal{A}'$ ne faisant intervenir ni l'addition ni la multiplication externe par un élément de k. On considérera une seconde structure $\mathcal{B}$, dépendant d'un domaine D de $\mathcal{A}$, incluant la structure d'espace vectoriel sur k et le fait que si D est un domaine de $\mathcal{A}$ et E un domaine de $\mathcal{B}(D)$, alors E est muni d'une structure $\mathcal{B}'(D)$. La structures $\mathcal{B}'(D)$ sur E fera intervenir des opérations internes $*_i$ $i \in [1, n]$, des applications internes f_i $i \in [1, m]$, et des opérations $\diamond_i$ $i \in [1, \ell]$ de $D \times E$ dans E. On notera (E) le sous-espace vectoriel engendré par E.

CONDITION 1. — *Les axiomes de $\mathcal{B}'$ impliquent l'existence d'un élément $\top$ et qu'on ait, pour tout domaine*

A de $\mathcal{A}'$ et tout domaine B de $\mathcal{B}'(A)$:

$$\begin{aligned}
&\forall i \in [1,m]\ f_i\top = \top,\\
&\forall i \in [1,n]\ \forall a \in B\ a *_i \top = \top *_i a = \top,\\
&\forall i \in [1,\ell]\ \forall (a,b) \in A \times B\ a \diamond_i \top = \top \diamond_i b = \top,\\
&\forall i \in [1,m]\ \forall (a,b) \in B^2\ \forall (\alpha,\beta) \in k^2\ f_i(\alpha a + \beta b) \in (f_i\, a, f_i\, b),\\
&\forall i \in [1,n]\ \forall (a,b,c) \in B^3 \forall (\alpha,\beta) \in k^2\ a *_i (\alpha b + \beta c) \in (a *_i b, a *_i c)\\
&\qquad \text{et } (\alpha a + \beta b) *_i c \in (a *_i c, b *_i c),\\
&\forall i \in [1,\ell]\ \forall (a,b,c,d) \in A^2 \times B^2\ \forall (\alpha,\beta) \in k^2\ a \diamond_i (\alpha c + \beta d) \in (a \diamond_i c, a \diamond_i d)\\
&\qquad \text{et } (\alpha a + \beta b) \diamond_i c \in (a \diamond_i c, b \diamond_i c).
\end{aligned}$$

Le rôle de l'élément $\top$ sur un domaine B de $\mathcal{B}$ ou $\mathcal{A}$ sera joué par l'élément $\mathbf{0}$.

Un morphisme ϕ d'un domaine B vers un domaine B' de $\mathcal{B}'(A)$ satisfera les axiomes suivants :

$$\begin{aligned}
&\forall (a,b) \in B^2\ \phi(a *_i b) = \phi(a) *_i \phi(b),\\
&\forall a \in B\ \phi f_i a = f_i \phi a,\\
&\forall (a,b) \in A \times B\ \phi(a \diamond_i b) = a \diamond_i \phi(b),\\
&\phi(\top_B) = \top_{B'}.
\end{aligned}$$

Définition 1. — *On appellera filtration sur un domaine A de $\mathcal{A}$, la donnée d'une application d'un domaine A' de $\mathcal{A}'$ dans $\mathcal{P}(A)$ $a \mapsto A_a$, telle que pour tout $(a,b) \in A' \times A'$:*

a) $A_a \subset A_b$ ou $A_b \subset A_a$,
b) $A_a + A_b \subset A_a \cup A_b$,
c) $kA_a = A_a$.
d) si $\bullet$ est une opération interne de la structure $\mathcal{A}'$, on ait $A_a \bullet A_b \subset A_{a \bullet b}$, $A_a \subset A_{a\bullet b}$ et $A_b \subset A_{a\bullet b}$.

On appellera filtration d'un domaine B de $\mathcal{B}(A)$, la donnée d'une filtration de A par un $\mathcal{A}'$-domaine A' et d'une application d'un $\mathcal{B}'(A')$-domaine B' dans $\mathcal{P}(B)$, $a \mapsto B_a$, telle que pour tout $(a,b) \in B' \times B'$:

e) $B_a \subset B_b$ ou $B_b \subset B_a$,
f) $B_a + B_b \subset B_a \cup B_b$,
g) $kB_a = B_a$,
h) (compatibilité avec la structure $\mathcal{B}'(A)$)

$$\begin{aligned}
&\forall i \in [1,\ell]\ \forall (a,b) \in A' \times B'\ A_a \diamond_i B_b \subset B_{a \diamond_i b}\\
&\qquad B_b \subset B_{a \diamond_i b},\\
&\forall i \in [1,m]\ \forall a \in B'\ f_i B_a \subset B_{f_i a}\\
&\qquad B_a \subset B_{f_i a},\\
&\forall i \in [1,n]\ \forall (a,b) \in B' \times B'\ B_a *_i B_b \subset B_{a *_i b}\\
&\qquad B_a \subset B_{a *_i b}\\
&\qquad B_b \subset B_{a *_i b}.
\end{aligned}$$

On considérera un domaine A de $\mathcal{A}$ filtré par A' et un domaine B de $\mathcal{B}'(A)$ filtré par B', sur lesquels on va imposer quelques conditions supplémentaires.

Condition 2. — *Il existe sur B' une relation d'ordre total $<$, compatible avec la filtration, c'est-à-dire telle que $B_a \subset B_b \Longleftrightarrow a \leq b$.*

Ceci revient à dire que $<$ est compatible avec la structure $\mathcal{B}'(A')$ de B, ou plus précisément avec le préordre provenant de la structure.

Définition 2. — *On notera $\ll$ le préordre provenant de la structure de B', qui est le plus petit ordre sur B tel que : a) $a \ll f_i a$ et $a \ll b$ implique $f_i a \ll f_i b$,*

b) $a \ll a *_i b$, $a \ll b *_i a$, $a \ll b$ implique $c *_i a \ll c *_i b$ et $a *_i c \ll b *_i c$,
c) $a \ll c \diamond_i a$ et $a \ll b$ implique $c \diamond_i a \ll c \diamond_i b$.

PROPOSITION 1. — *On a $a \ll b$ implique $a \leq b$.* ■

CONDITION 3 (Condition de chaîne descendante). — *Pour toute famille $(a_i)_{i\in\mathbf{N}}$ d'éléments de B' telle que $a_i \leq a_j$ si $i \leq j$, il existe un entier p tel que $a_i = a_p$ pour tout $i \geq p$.*

Remarques. — 1) Une conséquence immédiate de cette propriété est que tout sous-ensemble de B' admet un élément minimal.

2) Ceci implique aussi que $\ll$ est un ordre.

DÉFINITION 3. — *On définit une application $\tau : B \mapsto B'$, qui à un élément non nul a de B associe le plus petit élément b de B' tel que $a \in B_b$. Par convention, on posera $\tau 0 = \top$*

On définit de manière identique une application $\tau : A \mapsto A'$.

CONDITION 4. — *L'application τ: $A \mapsto A'$ est surjective.*

On peut donc se donner une application μ: $A' \mapsto A$, telle que $\tau \circ \mu = \mathrm{Id}_{A'}$. On supposera par la suite qu'une telle application a été choisie. On se donne de même une application μ: $\tau(B) \mapsto B$ satisfaisant $\tau \circ \mu = \mathrm{Id}_{\tau(B)}$.

DÉFINITION 4. — *On définit une application* tête: $B \mapsto B$ *par* tête $a = \mu \circ \tau$.

CONDITION 5. — *Soient a et b deux éléments de $B_\star$ (resp. $A_\star$), alors si $\tau a = \tau b$, il existe $(\alpha, \beta) \in k_\star^2$, unique à un coefficient près tel que $\alpha a + \beta b = 0$ ou $\tau(\alpha a + \beta b) < \tau a$. Si $\tau a > \tau b$, alors $\tau(a + b) = \tau a$.*

En d'autres termes, $\bigcup_{a'<a} B_{a'}$ est un sous-espace vectoriel de codimension 1 de B_a.

DÉFINITION 5. — *Si a est un élément non nul de B ou A, on notera $\kappa(a)$ l'élément α de $k_\star$ tel que $\tau(a - \alpha \text{tête}\, a) < \tau a$.*

PROPOSITION 2. — *Si $\tau a = \tau b$, et si $\kappa a = -\kappa b$, alors $\tau(a + b) < \tau a$.*

PREUVE. $\tau(a + b) = \tau\big((a - \kappa a \text{tête}\, a) + (b - \kappa b \text{tête}\, b)\big)$. ■

On retrouve la situation des bases standard d'idéaux sur $k[n]$, en prenant pour tête l'application monôme dominant et pour κ l'application coefficient dominant.

CONDITION 6. — *Pour tout domaine D' de $\mathcal{B}'(C')$, les sous-domaines E de D' sont caractérisés par les conditions de stabilité suivantes :*

$$
\begin{aligned}
E *_i E &\subset \ E \ i \in [1, n],\\
C' \diamond_i E &\subset \ E \ i \in [1, \ell],\\
f_i(E) &\subset \ E \ i \in [1, m].
\end{aligned}
$$

Si E est un sous-$\mathcal{B}'(C)$-domaine d'un domaine D de $\mathcal{B}(C)$, le s.-e.v. engendré par E est un domaine de $\mathcal{B}(C)$.

Lemme 1. — *Si $\mathcal{B}$ (resp. $\mathcal{B}'$) vérifie la condition 6, alors pour tous sous-domaines D et E d'un domaine C de $\mathcal{B}$ (resp. $\mathcal{B}'$), $D \cap E$ est un sous-domaine de C.* ■

DÉFINITION 6. — *On appellera sous-domaine d'un domaine D de $\mathcal{B}(C)$ (resp. $\mathcal{B}'(C')$) engendré par un sous-ensemble E de D et l'on notera $[E]_{\mathcal{B}}$ (resp $[E]_{\mathcal{B}'}$)* [5] *le plus petit sous-ensemble de D satisfaisant les axiomes de $\mathcal{B}(C)$ (resp. $\mathcal{B}'(C')$) et contenant E.*

PROPOSITION 3. — *Si la condition 6 est vérifiée, alors pour tout sous-ensemble E d'un domaine D de $\mathcal{B}(C)$ (resp $\mathcal{B}'(C')$), $[E]_D$ existe et est l'intersection de tous les sous-domaines de D contenant E.* ■

On va effectuer une construction, qui peut s'avérer essentielle pour certaines généralisations, en particulier pour les bases standard d'idéaux différentiels en caractéristique positive. Elle est triviale et inutile si τ est un morphisme.

[5] On pourra aussi noter $[E]_D$ lorsqu'il y aura une ambiguïté sur le domaine de base et non sur la structure.

DÉFINITION 7. — *On va redéfinir les opérations et fonction de la structure $\mathcal{B}'(A')$ sur B' de la manière suivante :*

$$\begin{aligned}
\forall i \in [1,\ell]\ \forall (a,b) \in A' \times B'\ a \diamond_i b &= a \diamond_i b \text{ si } \forall (c,d) \in A \times B\ \tau c = a \text{ et } \tau d = b \\
&\qquad\qquad \Longrightarrow \tau(c \diamond_i d) = a \diamond_i b \\
&= \top \text{sinon}, \\
\forall i \in [1,m]\ \forall a \in B'\ f_i a &= f_i a \text{ si } \forall b \in B\ \tau b = a \Longrightarrow \tau f_i b = f_i a \\
&= \top \text{sinon}, \\
\forall i \in [1,n]\ \forall (a,b) \in B' \times B'\ a *_i b &= a *_i b \text{ si } \forall (c,d) \in B^2\ \tau c = a \text{ et } \tau d = b \\
&\qquad\qquad \Longrightarrow \tau(c *_i d) = a *_i b \\
&= \top \text{sinon}.
\end{aligned}$$

B' muni des opérations ainsi redéfinies sera noté B''.

CONDITION 7. — *B'' possède la structure $\mathcal{B}'(A')$.*

CONDITION 8. — *Pour tout ensemble E, il existe un $\mathcal{B}'(A')$-domaine libre construit sur E, c'est-à-dire un domaine L contenant E tel que pour toute application h de E dans un domaine D, il existe un morphisme ϕ de L dans D rendant le diagramme suivant commutatif :*

$$\begin{array}{ccc}
E & \hookrightarrow & L \\
 & \searrow h & \downarrow \phi \\
 & & D.
\end{array}$$

Nous noterons ce domaine $\mathbf{L}(E)$.

Il faut encore imposer une condition supplémentaire.

CONDITION 9. — *B muni des opérations $*_i$, des fonctions f_i et des opérations externes $\diamond_i : A' \times B \mapsto B$ définies par $a \diamond_i b = \mu(a) \diamond_i b$, possède la structure $\mathcal{B}'(\mathcal{A}')$, en prenant 0 pour élément $\top$.*

Cette supposition peut paraître un peu excessive, mais en fait on ne se sert pas du tout de la structure interne de A, mais seulement des opérations externes $\diamond_i$, ce qui permet en pratique d'adopter pour $\mathcal{A}'$ une structure réduite, voire vide, ce qui augmente les chances de satisfaire la condition 9.

DÉFINITION 8. — *Si E est un sous-ensemble de B, on notera ϕ le morphisme de $\mathbf{L}(E)$ dans B, correspondant à l'injection canonique, ϕ' et ϕ'' les morphisme de $\mathbf{L}(E)$ dans B' et B'' correspondant à τ.*

Lemme 2. — *Si E est un sous-ensemble de B, alors $[E]_{\mathcal{B}'(A')} = \phi\mathbf{L}(E)$, $[\tau E]_{B'} = \phi'\mathbf{L}(E)$ et $[\tau E]_{B''} = \phi''\mathbf{L}(E)$.* ∎

PROPOSITION 4. — *Si E est un sous-ensemble de B, et e un élément de $\mathbf{L}(E)$ tel que $\phi'' e \neq \top$, alors $\tau\phi e = \phi' e$.* ∎

COROLLAIRE 1. — *Soient E un sous-ensemble de B et b un élément de $[\tau E]_{B''}$, alors il existe $a \in [E]_{\mathcal{B}'}$ tel que $\tau a = b$*

PREUVE. Si $b = \top$, c'est immédiat en prenant 0 pour a. On effectue alors un raisonnement par l'absurde. On considère l'ordre $\ll$ provenant de la structure de $D = [\tau E]_{B''}$.

Pour $b \neq \top$ c'est une conséquence immédiate de la proposition. ∎

Dans la suite du paragraphe, nous supposerons systématiquement que ces conditions sont vérifiées, et nous utiliserons les mêmes notations.

2. Bases standard

Nous allons caractériser les sous-domaines de B, en leur associant des sous-ensembles privilégiés, que nous appellerons *bases standard*.

DÉFINITION 9. — *Soit C un sous-domaine de B, on appelle base standard de C un sous-ensemble G de C tel que $[\tau(G)]_{B''} = \tau(C)$.*

Cette définition est purement formelle. Nous allons monter qu'on retrouve effectivement certaines propriétés des bases standard d'idéaux.

DÉFINITION 10 (Réduction). — *Soient E un sous-ensemble de B, a et b deux éléments de B, on dit que a est élémentairement réduit à b par E si $a \neq 0$ et s'il existe $c \in [\tau E]_{B''}$, $d \in [E]_{B'(A')}$ tel que $\tau d = \tau a = c$ et $b = a - \kappa a / \kappa c c$. On notera alors $a \xrightarrow{E} b$ et l'on dira que a est réductible par E s'il existe b tel que $a \xrightarrow{E} b$.*

On dira que a est réduit à b par E s'il existe une chaîne de réductions élémentaires finie

$$a = x_0 \xrightarrow{E} x_1 \xrightarrow{E} \cdots \xrightarrow{E} x_{p-1} \xrightarrow{E} x_p = b.$$

On notera $a \xrightarrow{E^\star} b$.

Enfin, on dira que a est absolument réduit à b par E si a est réduit à b par E et pour tout c tel que $a \xrightarrow{E} c$, il existe b' tel que $c \xrightarrow{E^\star} b'$ et $\tau b' = \tau b$. On notera $a \xRightarrow{E} b$.

Lemme 3. — *Si $a \xrightarrow{E} b$, et $b \neq 0$ alors $\tau(a) > \tau(b)$.* ∎

PROPOSITION 5. — *Toute chaîne de réductions élémentaires est finie.*

PREUVE. Ceci résulte de la propriété de chaîne descendante et du lemme. ∎

PROPOSITION 6. — *a est irréductible par rapport à E ssi $\tau a \notin [\tau E]_{B''}$.*

a est réduit à 0 par E ssi il existe $\alpha \in k^p$ et $e \in \mathbf{L}(E)^p$ tels que $\phi' e_i > \phi' e_j$ $i > j$ $\phi'' e_i \neq 0$ et $a = \sum_{i=1}^p \alpha_i \phi e_i$. ∎

THÉORÈME 1. — *Les propriétés suivantes sont équivalentes :*

i) G est une base standard de C,

ii) G est un sous-ensemble de C et tous les éléments non nuls de C sont réductibles par G.

iii) G est un sous-ensemble de C et tous les éléments de C sont absolument réduits à 0 par G.

iv) $\forall a \in B$ $a \in C \Longleftrightarrow a \xrightarrow{G^\star} 0$.

PREUVE. ∎

On voit d'après l'assertion iv) du théorème qu'une base standard caractérise le sous-domaine qu'elle engendre. En revanche, un même domaine peut avoir plusieurs bases standards distinctes. On peut montrer que la structure de corps de k et la condition de chaîne descendante impliquent l'existence de bases standard minimales et sous une hypothèse supplémentaire d'une unique base standard réduite.

PROPOSITION 7. — *Tout sous-domaine D de B'' admet un ensemble minimal de générateurs.*

PREUVE. Soit E l'ensemble des éléments de D minimaux pour le préordre $\ll$ induit par la structure. On va montrer que E engendre D. Supposons qu'un élément a de D n'appartienne pas à $[E]_D$. Alors a n'est pas minimal pour $\ll$. Trois cas peuvent se produire :

a) $\exists i \in [1, m]$ $\exists b \in D$ $a \neq b$ et $a = f_i(b)$,

b) $\exists i \in [1, \ell]$ $\exists b \in D$ $\exists c \in A'$ $a \neq b$ et $a = c \diamond_i b$,

c) $\exists i \in [1, n]$ $\exists (b, c) \in (D \setminus \{a\})^2$ $a = b *_i c$.

Dans les cas a) et b), l'hypothèse implique que $b \notin [E]_D$. Dans le cas c), elle implique que b ou c n'appartiennent pas à $[E]_D$. Donc, pour tout élément a de $D \setminus [E]_D$, il existe $d \in D \setminus [E]_D$ $d \ll a$. On peut donc par récurrence construire une chaîne infinie strictement décroissante d'éléments de D, ce qui contredit la propriété de chaîne descendante. ∎

DÉFINITION 11. — *On appelle base standard minimale d'un sous-domaine C de B une base standard G telle que $\tau(G)$ est l'ensemble minimal de générateurs de $\tau(C)$.*

PROPOSITION 8. — *Tout sous-domaine D de B admet une base standard minimale.*

PREUVE. Soit E l'ensemble minimal de générateurs de $\tau(D)$ dans B''. Pour tout élément e de E, on peut choisir un élément e' de D tel que $\tau(e') = e$. L'ensemble de ces éléments constitue manifestement une base standard minimale. ∎

DÉFINITION 12. — *On dira alors que a est unitaire si $\kappa a = 1$.*

Il existe manifestement pour tout $a \in B_\star$ un unique élément unitaire b tel que $b = \alpha a$ pour $\alpha \in k$. Cet élément sera noté unit a.

DÉFINITION 13. — *On appelle reste d'un élément a de B, l'élément* $\operatorname{reste}(a) = a - \kappa(a)\mu \circ \tau a$ *si* $a \neq 0$ *et* 0 *sinon. On dira que a est élémentairement totalement réduit à b par E si a est réduit à b par E ou bien s'il existe c tel que* $\operatorname{reste} a \xrightarrow{E} c$ *et* $b = \kappa a \text{tête}\, a + c$. *On dira alors que a est totalement réduit à b par E s'il existe une chaîne de réductions totales élémentaires de a vers b. S'il n'existe pas d'élément b différent de a tel que* $a \xrightarrow{E_{\mathrm{tot}}} b$, *on dira que a est totalement irréductible par E.*

Lemme 4. — *Il n'existe pas de chaîne infinie de réductions totales élémentaires.* ∎

Lemme 5. — *Si S et S' sont deux bases standard de $D \subset B$, si* $a \xrightarrow{S_{\mathrm{tot}}} b$, $c \xrightarrow{S'_{\mathrm{tot}}} d$, *où* $a - c \in D$ *et si b et d sont réduits par rapport à S et S', alors* $\tau b = \tau c$ *et* $\kappa b = \kappa c$.

PREUVE. Comme $b - d \in D$, $\tau(b - d) < \tau b$, sinon b serait réductible ; d'où le lemme. ∎

PROPOSITION 9. — *Si G est une base standard de $D \subset B$, alors pour tout a dans B il existe un unique élément b tel que* $a \xrightarrow{G_{\mathrm{tot}}} b$ *et b est totalement irréductible par G. Il ne dépend pas de la base standard choisie. On notera cet élément* $\operatorname{red}_D(a)$.

L'ensemble des éléments totalement irréductibles de B par rapport à D forme un espace vectoriel V tel que $B = D \oplus V$ *et* $V = \operatorname{red}_D(B)$.

PREUVE. Pour la première partie, il suffit de montrer que si S et S' sont deux bases standard de D, $a \xrightarrow{S_{\mathrm{tot}}} b$ et $a \xrightarrow{S_{\mathrm{tot}}} c$ avec b et c totalement irréductibles par rapport à S et S' respectivement, alors $b = c$. D'après le lemme, $\tau b = \tau c$ et $\tau(b - c) < \tau b$. Si $\tau \operatorname{reste} b > \tau(b - c)$ et $\tau \operatorname{reste} c > \tau(b - c)$, $\tau \operatorname{reste} b = \tau \operatorname{reste} c$ et $\kappa \operatorname{reste} b = \kappa \operatorname{reste} c$. Par récurrence, on voit qu'il existe un entier i tel que $\tau \operatorname{reste}^{i+1}(b \text{ ou } c) \leq \tau(b - c)$, $\tau \operatorname{reste}^i b > \tau(b - c)$ et $\tau \operatorname{reste}^i c > \tau(b - c)$. Ceci implique $\tau \operatorname{reste}^{i+1}(b \text{ ou } c) = \tau(b - c)$ et donc b ou c réductible ; contradiction.

Pour la seconde partie, montrons d'abord que $B = D + V$. Soit $a \in B$, $a - \operatorname{red}_D(a) \in D$ et $\operatorname{red}_D a \in V$ donc $a \in D + V$. Il est maintenant manifeste que $V \cap D = \{0\}$. ∎

COROLLAIRE 1. — *Pour tout $D \subset B$ il existe une unique base standard minimale G de D composée d'éléments unitaires dont le reste est totalement réduit par rapport à D.* ∎

3. Syzygies

DÉFINITION 14 (Congruences). — *Soient D un $\mathcal{B}'(A')$-domaine, on appelle congruence sur D un sous-ensemble C de D^2 tel que* $\forall (a, b) \in C$

$$\begin{aligned} (f_i a, f_i b) &\in C, \\ \forall c \in D (c *_i a, c *_i b) &\in C \\ \text{et } (a *_i c, b *_i c) &\in C, \\ \forall c \in A' (c \diamond_i a, c \diamond_i b) &\in C, \end{aligned}$$

et tel que C soit une relation d'équivalence.

PROPOSITION 10. — *Si C et C' sont deux congruences sur un $\mathcal{B}'(A')$-domaine D, alors $C \cap C'$ est une congruence.*

Si $\pi \colon D \mapsto D'$ *est un morphisme de $\mathcal{B}'(A')$-domaines, l'ensemble* $\{(a, b) \in D^2 | \pi(a) = \pi(b)\}$ *est une congruence sur D.* ∎

DÉFINITION 15. — *On appellera congruence engendrée par une partie E de D^2 la plus petite congruence sur D contenant E.*

DÉFINITION 16 (Syzygies). — *Soient E un sous-ensemble de B, et* $L_E = \mathbf{L}_{\mathcal{B}'(A')}(E)$, *on note ϕ l'application canonique de L_E dans B et ψ l'application canonique de L_E dans B'' correspondant à l'application τ.*

On appelle ensemble des syzygies entre éléments de L_E la congruence associée au morphisme ψ, et ensemble des syzygies entre éléments de E l'image par ϕ de l'ensemble des syzygies entre éléments de L_E. Le S-élément associé à une syzygie (a, b) entre éléments de E sera l'élément $\operatorname{unit}(\kappa(b)a - \kappa(a)b)$, *si* $a, b \neq 0$ *et* $\operatorname{unit} a$ *(resp.* $\operatorname{unit} b$*) si* $b = 0$ *(resp.* $a = 0$*).*

Il convient d'apporter quelques précisions sur ces syzygies "non homogènes", faisant intervenir 0. Dès lors que la connaissance des termes de tête de a et b n'est plus suffisante pour connaître avec certitude le terme de tête de $a *_i b$ [(6)], on a redéfini $\tau a *_i \tau b$ par $\top$, ceci a pour effet de faire apparaître la syzygie $(a *_i b, 0)$ et oblige à considérer $a *_i b$ comme un S-polynôme, de sorte qu'on ne perd pas d'information en chemin.

On se donne un préordre $\prec$ sur B', compatible avec la structure, et tel que $<$ soit compatible avec $\prec$.

DÉFINITION 17. — *On dira que deux éléments a et b de B sont de même rang si l'on a à la fois $\tau(a) \preceq \tau(b)$ et $\tau(b) \preceq \tau(a)$. On appellera rang de a $(\mathrm{rg}(a))$ la classe d'équivalence des éléments de A' de même rang que a.*

Le rang d'une syzygie (a, b) entre éléments de L_E sera le maximum des rang de $\psi' a$ et $\psi' b$, en notant ψ' le morphisme canonique de L_E dans B'.

Si (a, b) est une syzygie entre éléments de L_E, telle que $a, b \neq \top$, et $\phi' a = \phi' b$, elle sera dite homogène, ainsi que la syzygie entre éléments de E qui lui correspond. Une syzygie sera dite quasi-homogène si elle est homogène, ou si elle est du type $(a, \top)$ ou $(a, 0)$.

Pour rendre praticable le calcul effectif d'une base standard, un point important est de détecter a priori un certain nombre de syzygie dont le S-élément est nul, ou se réduit à 0.

DÉFINITION 18. — *On dira qu'un ensemble S de syzygies entre éléments de L_E est négligeable si pour tout $(a, b) \in \phi S$ le S-élément associé est réduit à 0 par E, où si S est contenue dans la congruence engendrée par un ensemble négligeable.*

On dira qu'un ensemble de S de syzygies quasi-homogènes entre éléments de L_E est essentiel s'il existe un ensemble négligeable S' de syzygies entre éléments de L_E tel que $S \cup S'$ engendre l'ensemble des syzygies entre éléments de L_E. L'image par ϕ d'un ensemble de syzygies essentiel entre élément de L_E sera qualifié d'ensemble de syzygie essentiel entre élément de E.

Si toutes les syzygies de rang au plus r sont contenues dans l'ensemble engendré par $S \cup S'$, on parlera d'un ensemble de syzygies r-essentiel.

La détermination effective d'un ensemble de syzygies négligeable est un problème qu'on ne peut pas aborder à ce niveau de généralité, puisqu'il dépend spécifiquement des propriétés de la structure en cause. Mais déjà le fait de se ramener à un ensemble de syzygies générateur permet, dans le cas des bases standard d'idéaux de polynômes, de retrouver la plupart des critères connus. Seul le critère permettant d'éliminer les syzygies entre polynômes dont les termes de tête sont étrangers relève spécifiquement de la structure. On verra un autre exemple de syzygies négligeables avec les bases standard d'idéaux différentiels.

DÉFINITION 19. — *Soit E un sous-ensemble de B et a un élément de $[E]_B$, on appelle taille de a par rapport à E le rang maximal des éléments $e_1, \ldots, e_p$ de L_E tel qu'il existe $\alpha_1, \ldots, \alpha_p$ vérifiant $a = \sum_{i=1}^{p} \alpha_i \phi e_i$.*

DÉFINITION 20. — *Soit E un sous-ensemble de B, on notera $[E]_r$ le plus petit sous-ensemble de B tel que $[E]_r$ contient tous les éléments de taille r par rapport à E et tous les éléments de taille r par rapport à $[E]_r$. On appelle altitude d'un élément a de $[E]_B$ par rapport à E, le plus petit r tel que $a \in [E]_r$.*

Pour fixer les idées, on peut dire de manière approximative que l'altitude de a est le rang maximal des calculs intermédiaires nécessaires pour obtenir a à partir des éléments de E en ne s'autorisant à utiliser que les opérations de la structure.

Lemme 6. — *Si E est un sous-ensemble de B, on note $B_{r,0}(E)$ le sous-espace vectoriel engendré par les éléments de $[E]_{\mathcal{B}'(A')}$ de rang inférieur où égal à r, et l'on pose $B_{r,n+1}(E) = B_{r,0}\left(B_{r,n}(E)\right)$. On a alors $[E]_r = \bigcup_{i=0}^{\infty} B_{r,i}(E)$.*

En outre, si tous les éléments de $B_{r,0}(E)$ sont réductibles par E, alors $[E]_r = B_{r,0}(E)$. ■

Lemme 7. — *Si E est un sous-ensemble de $D \subset B$ tel que tout les éléments de taille strictement inférieure à r soient réduits à 0 par E et s'il existe un ensemble r-essentiel de syzygies entre éléments de E tel que tous les S-éléments associés sont réduits à 0 par E, alors le S-élément associé à toute syzygie de rang au plus r est réduit à 0 par E* ■

(6) Déjà un problème d'identifiabilité !

THÉORÈME 2. — *Les propriétés suivantes sont équivalentes :*

i) G est une base standard du sous-domaine D de B,

ii) $D = [G]$ et tous les S-éléments associés à un ensemble essentiel de syzygies entre éléments de G sont réduits à 0 par G.

PREUVE. i)$\Longrightarrow$ii) est immédiat, puisque les S-éléments appartiennent à D.

ii)$\Longrightarrow$i) va résulter d'un théorème plus précis.

THÉORÈME 3. — *Soit $D \subset B$ un sous-domaine de B, E un sous-ensemble générateur de D et S un r-ensemble essentiel de syzygies entre éléments de E, alors si tous les S-éléments provenant de S se réduisent à 0, tous les éléments d'altitude au plus r sont absolument réduits à 0 par E.*

PREUVE. D'après le lemme 6, il suffit de prouver que tous les éléments non nuls de $B_{r,0}(E)$ sont réductibles par E. Supposons ce résultat faux. Pour les besoins de la démonstration, on considère momentanément le rang par rapport à $<$ et l'on choisit parmi les éléments de B de taille minimale qui ne le satisfont pas un élément a tel que

$$a = \sum_{i=1}^{p} \alpha_i \phi e_i \text{ avec } \alpha_i \in k,\ e_i \in \mathbf{L}(E) \operatorname{rg} e_i \leq r,$$

avec p minimal. Le rang de a par rapport à $\prec$ est inférieur à r.

Tous les éléments de rang strictement plus petit que a sont réductibles par E, ce qui implique, par récurrence qu'ils sont réduits à 0 par E.

On commence par envisager le cas $p = 1$. Si $\phi'' e_1 \neq \top$, a est réductible, donc $\phi'' e_1 = \top$. Mais alors, a est un S-élément et se réduit à 0 d'après le lemme 7 ; contradiction.

On peut donc supposer $p > 1$. $b' = \alpha_1 e_1$ et $b'' = \sum_{i=2}^{p} \alpha_i e_i$ sont réductibles. On a donc $b' = \sum_{i=1}^{p'} \alpha'_i \phi e'_i$ et $b'' = \sum_{i=1}^{p''} \alpha''_i \phi e''_i$, où les α'_i, e'_i, etc. satisfont les conditions de la prop. 2.6 p. 45. Nécessairement, $\alpha'_1 \kappa \phi e'_1 = -\alpha''_1 \kappa \phi e''_1$ et $\phi'' e'_1 = \phi'' e''_1 \neq 0$. On en déduit que $b''' = \alpha'_1 e'_1 + \alpha''_1 e''_1$ est un multiple d'un S-élément et qu'il est donc réduit à 0 par E. Cette réduction donne une décomposition $\sum_{i=1}^{p'''} \alpha_{i'''} \phi e_{i'''}$ de b''' avec $\phi'' e'''_1 < \tau a$. Donc

$$a = \sum_{i=2}^{p'} \alpha'_i \phi e'_i + \sum_{i=2}^{p''} \alpha''_i \phi e''_i + \sum_{i=1}^{p'''} \alpha_{i'''} \phi e_{i'''},$$

où les e'_i, e''_i et $e_{i'''}$ sont tous de rang strictement inférieur à la taille de a ; contradiction. ∎

4. Procédures de complétion

Il faut renforcer une dernière fois les hypothèses, pour qu'on puisse définir des méthodes effectives de construction.

CONDITION 10 (Effectivité). — *On suppose que k, A, B, A' et B' sont effectifs, que les applications τetκ le sont et que pour tout sous-ensemble fini de E on dispose d'un algorithme permettant d'énumérer les éléments d'un ensemble essentiel de syzygies entre éléments de E, ainsi qu'un algorithme permettant de tester l'appartenance d'un élément à $[\tau E]_{B''}$.*

On pourrait alors montrer qu'une procédure de complétion peut être donnée, pour les sous-domaines de type fini. Comme en général, les bases standard seront infinies, et que l'ensemble syzygies à considérer peut être lui-même infini, la procédure ne s'arrêtera pas en général, même si une base standard finie existe. Mais elle pourra retourner à chaque boucle un ensemble G_i, et la convergence de la procédure signifiera que $\bigcup_{i=1}^{\infty} G_i$ est une base standard.

À ce niveau de généralité, cela ne présente pas un grand intérêt. Mieux vaut définir ces procédures dans chaque cas particulier, de manière à les rendre aussi efficaces que possible. On verra au chap.IV § 1 n° 2.4 un exemple d'une telle procédure, adapté au cas des bases standard d'idéaux différentiels. En outre, dans le cas des bases canoniques, ou bases standard de sous-algèbre, on donnera au § 3 n° 3.2 une procédure de complétion qui s'arrête ssi la base canonique est finie, car dans ce cas il n'y a toujours qu'un nombre fini de S-polynômes à considérer, pourvu que la sous-algèbre soit finiment engendrée.

§ 2. SOUS-ALGÈBRES ET SOUS-CORPS

Étant donné un ordre admissible sur les monômes de $k[n]$, on notera $\mathrm{m}(P)$ le monôme dominant de P. Par la base standard d'un idéal, on entendra son unique base standard réduite.

1. Méthode du graphe

Nous allons décrire une méthode permettant de tester l'appartenance d'un polynôme à une sous-algèbre de $k[n]$, ou plus généralement, étant donnée $A \subset B$, deux sous-algèbres de $k(n)$ de tester si une fraction donnée de B appartient à A. Cette méthode nécessite le calcul d'une seule base standard, à partir de laquelle une réponse pourra être obtenue pour chaque candidat par une simple réduction. Dans le cas ou l'on souhaite tester qu'une fraction quelconque est ou non dans A, il faudra éventuellement élargir B et calculer une nouvelle base standard. Cette méthode est celle donnée par SHANNON et SWEEDLER dans [SS], auquel on se reportera pour de plus amples détails.

DÉFINITION 1. — *Un ordre admissible sur les monômes de $k[x_1, \dots, x_n, y_1, \dots, y_m]$ est un ordre d'élimination pour les x, si pour tout indice i $x_i > y^\alpha$. On dit que c'est un ordre d'élimination forte si $x^\alpha > x^\beta \Longrightarrow x^\alpha > x^\beta y^\gamma$.*

On dira qu'un ordre sur $k[x, y, z]$ élimine (fortement) les x puis les y si c'est un ordre d'élimination (forte) pour les x et pour $x \cup y$.

THÉORÈME 1. — *Soient $B = k[x_1, \dots, x_n, Q_1^{-1}, \dots, Q_m^{-1}]$ une sous-algèbre de $k(n)$. Soit $A = k[F_1, \dots, F_r]$ une sous-algèbre de B. Soit $\mathcal{I}$ l'idéal*

$$(Q_i(x)D_i - 1; i \in [1, m], T_i - F_i(x, D); i \in [1, r])_{k[x_1, \dots, x_n, D_1, \dots, D_m, T_1, \dots, T_r]},$$

et G une base standard de $\mathcal{I}$ relative à un ordre d'élimination pour les x puis les D. Alors $P = S(x, Q^{-1})$ est dans A ssi $S(x, D) \xrightarrow{G} R(T)$. De plus, on a $S = R(F)$.

PREUVE. D'après le th. II.5.1.1 p. 37, on sait qu'un polynôme de la forme $S(x, D) - R(T)$ appartient à l'idéal. Réduisant S par la base standard, l'ordre choisi est tel qu'on doive nécéssairement trouver un polynôme qui ne dépend que de T. ∎

Remarques. — 1) Si l'on souhaite tester l'appartenance d'une fraction donnée $P(x)/Q(x)$, il suffit de calculer la base standard de $\mathcal{I}$ en prenant $m = 1$ et $Q_1 = Q$. Mais il faudra en général répéter le processus à chaque introduction d'un nouveau dénominateur.

2) On peut noter que $\mathcal{I}' = \mathcal{I} \cap k[T]$ définit l'image de l'application rationnelle associée à F, et que A est isomorphe à $k[T]/\mathcal{I}'$.

3) Si l'on souhaite s'assurer que l'application rationnelle définie par F admet un inverse à gauche polynomial, il suffit de vérifier que pour tout $i \in [1, n]$ il existe dans G un polynôme de la forme $x_i - R_i(T)$.

Cette méthode ne s'étend pas en général pour tester l'appartenance d'une fraction à un sous-corps, à moins de recommencer pour chaque candidat un calcul de base standard.

THÉORÈME 2. — *Une fraction P/Q appartient au sous-corps $k(f_1, \ldots, f_m)$ où $f_i = P_i/Q_i \in \mathrm{Fr}k[x_1, \ldots, x_n]/\mathcal{I}$ ssi la base standard G de l'idéal*

$$\mathcal{J} = (\mathcal{I}; QW - P, Q_i(x)u_i - 1; i \in [1, m], T_iQ_i - P_i(x); i \in [1, r])_{k[u_1,\ldots,u_m,x_1,\ldots,x_n,W,T_1,\ldots,T_m]},$$

pour un ordre qui élimine $u \cup x$ puis élimine fortement W, contient un polynôme de la forme $R(T)W - S(T)$ où $R \notin \mathcal{I}$.

PREUVE. D'après la prop. II.4.1.2 p. 35, un tel polynôme doit appartenir à l'idéal. Ceci implique qu'il soit réduit par la base standard. Sans restriction de généralité, on peut remplacer R et S par leurs réductions totales par G. Maintenant, le polynôme ne peut pas être réduit par un élément de la base standard dont le terme de tête ne dépend que de T, puisque R est irréductible, pas plus que par un polynôme dont le terme de tête fait intervenir les x et les u, ou W à un exposant plus grand que 1. Ceci implique qu'il existe dans la base standard un polynôme dont le terme de tête est de la forme $\mathrm{m}(T)W$. Comme la base standard est réduite, il a nécessairement la forme voulue. ∎

COROLLAIRE 1. — *On considère une variété algébrique $X \subset \mathbf{A}^n$, définie par un idéal premier $\mathcal{I}$ et une application rationnelle f de X dans $\mathbf{A}^m$ définie par m fractions $F_i = P_i/Q_i$. Soit $\mathcal{J}$ l'idéal*

$$(\mathcal{I}, Q_i(x)u_i - 1, Q_i(x)T_i - P_i(x))_{k[u,x,T]}$$

et G la base standard réduite de $\mathcal{J}$ pour un ordre qui élimine les u, puis élimine successivement et fortement $x_1, \ldots, x_n$, alors f est inversible ssi, pour tout x_i, G contient un polynôme de la forme $S_i(T)x_i - R_i(T)$.

PREUVE. On commence par remarquer que $G \cap k[x, T]$ est la base standard du graphe, puisque l'ordre élimine les u. Manifestement, si $S_i(T)x_i - R_i(T)$ est dans la base standard, S_i n'appartient pas à $\mathcal{I}$. D'après la proposition II.4.1.1 cor. 3 p. 34, il en résulte que f est inversible.

Réciproquement, d'après le théorème, des polynômes de la forme souhaitée doivent appartenir à l'idéal. La propriété de l'ordre et le fait que la base standard est réduite impliquent alors que des polynômes de cette forme sont dans la base standard. ∎

2. Idéal Σ

On va donner une autre méthode permettant de conclure dans le cas de quelques sous-algèbres particulières de $k[n]$.

PROPOSITION 1. — *Soit A une sous-algèbre de $k[n]$ telle que $k(A) \cap k[n] = A$ et G une base standard de l'idéal $\Sigma(A)$, alors pour tout polynôme P de $k[n]$, $P \in A$ ssi $P(x) - P(y)$ est réduit à 0 par G.*

PREUVE. C'est une conséquence immédiate de la prop. II.5.2.1 p. 37. ∎

Remarques. — 1) On pourrait aussi utiliser un ordre qui élimine les x et tester que $P(x)$ est réduit à $P(y)$ par la base standard, mais cette méthode est sans doute moins intéressante en pratique, car elle exige de recourir à un ordre d'élimination.

2) Si $A = k[P_1, \ldots, P_m]$ est de type fini, $\Sigma(A) = (P_i(x) - P_i(y))$, la méthode est alors parfaitement effective.

3) On constate que l'idéal associé par cette méthode à une sous-algèbre ne dépend pas du système de générateurs choisi. Par noetherianité, on voit qu'on peut associer à toute sous-algèbre A coïncidant avec $k(A) \cap k[n]$ un nombre fini de polynômes engendrant $\Sigma(A)$. Le problème serait de les déterminer effectivement. On aurait alors un moyen de tester l'appartenance à ces algèbres, même lorsqu'elles sont de type infini. Ceci s'applique par exemple aux algèbres d'invariant sous l'action d'un groupe.

Proposition 2. — *Si f est une application polynomiale de A^n dans A^m, f est injective ssi pour tout $i \in [1, n]$ la base standard de l'idéal $(\Sigma(f),\ u(x_i - y_i) - 1)_{k[x,y,u]}$ est $\{1\}$.*

preuve. C'est une conséquence de la prop. II.5.2.2 p. 38. ∎

Proposition 3. — *Si f est une application polynomiale de A^n dans lui-même, f est polynomialement inversible ssi la base standard de $\Sigma(f)$ est de la forme $\{\epsilon_i(x_i - y_i)\}$ avec $\epsilon_i = \pm 1$.*

preuve. C'est la conséquence de la prop. II.5.2.2 cor. 1 p. 38. ∎

3. Idéal Δ

On décrit ici, une dernière méthode qui semble en pratique la plus efficace pour tester l'appartenance d'une fraction à un sous-corps et tester l'inversibilité. Si l'on travaille sur une variété X différente de $\mathbf{A}^n$, définie par un idéal $\mathcal{I}$, il faut supposer qu'on peut calculer dans $\mathrm{Fr}k[n]/\mathcal{I}$, le problème étant le test d'égalité à 0. Celui-ci est résolu si l'on connaît une base standard de $\mathcal{I}$, pour un ordre arbitraire. Au vu des calculs de base standard qui seront de toute façon nécessaires, cette supposition n'a rien d'excessif.

Théorème 3. — *Soit $g, f_1, \ldots, f_m$ des fractions de $K(X) \simeq \mathrm{Fr}k[n]/\mathcal{I}$, avec $g = P/Q$ et $f_i = P_i/Q_i$, G une base standard de l'idéal*

$$\mathcal{J} = (\mathcal{I}; \mathrm{ppcm}(Q_i(x))u - 1; Q_i(y)P_i(x) - P_i(y)Q_i(x))_{\mathbf{K}(X)[u,x]},$$

pour un ordre quelconque, alors $g \in k(f)$ ssi $Q(y)P(x) - P(y)Q(x)$ est réduit à 0 par G.

preuve. D'après la proposition II.4.2.5 p. 36, g appartient à $k(f)$ ssi ce polynôme est dans l'idéal $\mathbf{K}(X)\Delta$, qui n'est autre que $\mathcal{J} \cap \mathbf{K}(X)[x]$. Ceci est naturellement équivalent au fait qu'il est réduit à 0 par la base standard G. ∎

Corollaire 1. — *Sous les mêmes hypothèses, f définit une application rationnelle inversible ssi la base standard réduite de $\mathcal{J}$ pour un ordre quelconque est*

$$\{x_i - y_i; u_i - \frac{1}{Q_i(y)}\}.$$

preuve. On sait que ces polynômes sont dans l'idéal, et comme celui-ci n'est pas trivial, il ne peuvent être réduits que par eux-mêmes. ∎

4. Complexité

Considérant le cas d'une application $f : \mathbf{A}^n \mapsto \mathbf{A}^m$, on va montrer qu'on peut déduire de cette méthode un algorithme de test dont la complexité en terme d'opérations sur le corps de base est polynomiale en $O((m+1)(\deg f)^{O(n^3)})$.

On doit tester que $x_i - y_i \in \mathcal{J}$. On peut homogénéiser les générateurs de $\mathcal{J}$ au moyen d'une variable supplémentaire x_0. Ils engendrent alors un idéal $\widetilde{\mathcal{J}}$ [7]. Notons D le maximum des degrés des générateurs de $\mathcal{J}$, qui est au plus $\deg f + 1$. En utilisant le nullstellensatz effectif de Kollár, on sait que $x_0^q(x_i - y_i x_0)^p \in \widetilde{\mathcal{J}}$, avec $\deg(x_0^q(x_i - y_i x_0)^p) \leq D^{n+1}$, si $D > 2$. Le calcul de la base standard de $\mathcal{J}$ jusqu'en degré D^{n+1} se ramène classiquement à la triangulation d'un système linéaire donné par une matrice

$$\begin{pmatrix} (A_1) & (0) & \cdots & (0) \\ (0) & (A_2) & \cdots & \vdots \\ \vdots & & \ddots & (0) \\ (0) & \cdots & (0) & (A_{D^{n+1}}) \end{pmatrix},$$

où les colonnes représentent les polynômes dans la base des monômes, les blocs, rectangulaires, correspondant aux ensembles des multiples des polynômes générateurs par des monômes, regroupés degré par degré. En notant $\binom{D^{n+1}+n}{n+1}$ par δ, la taille de cette matrice est $\delta \times (m+1)\delta$ au plus. Un algorithme de base standard revient à trianguler cette matrice supérieurement en agissant sur les colonnes. Le coût est en $O((m+1)^3\delta^3)$ opérations sur le corps de fraction. Reste à majorer le coût des opérations sur le corps de base.

On peut remarquer que les coefficients des générateurs sont en fait des polynômes de $k[y]$, de degré borné par D. Utilisant pour la triangulation la méthode de Bareiss, les coefficients intermédiaires seront des mineurs de la matrice. On peut donc majorer leur degré par $D\delta$. Le coût des opérations élémentaires sur le corps de base est donc polynomial en le nombre de monômes des coefficients $\binom{D\delta+n}{n}$. Ayant construit la base standard jusqu'au degré nécessaire, il est évident de tester que les polynômes attendus sont bien dans l'idéal. On en déduit le résultat suivant.

Théorème 4. — *On peut tester que f admet un inverse à gauche rationnel en un nombre d'opérations sur le corps de base polynomial en*

$$\binom{D\delta+n}{n}(m+1)\delta = O\left((m+1)(\deg f)^{O(n^3)}\right).$$

■

Remarque 1. — Pour pouvoir contrôler la taille des coefficients, on a du opter pour un algorithme de triangulation particulier, qui peut s'interprèter comme un algorithme de base standard. Mais ceci signifie qu'on ne peut pas obtenir un résultat du même ordre pour n'importe quel algorithme de complétion, du moins pas avec cette méthode de démonstration.

---

[7] On utilise cette notation par commodité, mais ce n'est pas nécessairement l'homogénéisé de $\mathcal{J}$.

Si l'on veut déterminer l'inverse d'une application polynomiale $f\colon \mathbf{A}^n \mapsto \mathbf{A}^n$, en utilisant le corollaire du th. 1.2 p. 50, on peut utiliser le théorème prouvé par Gabber pour majorer la complexité des calculs. L'idéal $\mathcal{J}$ est engendré par les polynômes $(P_i(x) - T_i)$; on peut en effet oublier les u_i puisque l'application est polynomiale. Il faut tester que des polynômes de la forme $S_i(T)x_i - R_i(T)$ appartiennent à l'idéal pour tout indice i. Comme les fractions P/Q expriment l'inverse, le degré des S_i et R_i est au plus $(\deg f)^{n-1}$.

On donne à la variable T_i un poids égal à $\deg P_i$. On peut alors homogénéiser les polynômes générateurs avec une variable supplémentaire x_0 de poids 1. On obtient un nouvel idéal $\widetilde{\mathcal{J}}$, qui est aussi premier — c'est également un graphe — et ne contient pas x_0. Pour tout $1 \leq i \leq n$, un polynôme de la forme $x_0^p(\widetilde{S_i(T)x_i} - R_i(x))$ appartient à $\widetilde{\mathcal{J}}$. La puissance p peut être prise égale à 0 puisque l'idéal est premier et ne contient pas x_0. Le degré du polynôme par rapport au système de poids choisi est majoré par $(\deg f)^n + 1$, dans le cas général, ou $(\deg f)^n$ si l'inverse est polynomial. Ceci implique que

$$S_i(T)x_i - R_i = \sum_{j=1}^{n} M(x,T)(P_i - T_i),$$

avec $\deg(M(x,T)(P_i - T_i) \leq (\deg f)^n$. Cette majoration vaut aussi pour le degré usuel.

On peut se ramener comme ci-dessus à une triangulation. La matrice a une taille bornée par $\delta \times 2n\delta$, en notant $\binom{(\deg f)^n + 1 + 2n}{2n}$ par δ. Comme ses coefficients sont déjà sur le corps de base, on en déduit le résultat suivant.

PROPOSITION 4. — *On peut déterminer l'inverse d'une transformation polynomiale birationnelle de $\mathbf{A}^n$, avec une complexité en terme d'opérations sur le corps de base en*

$$O\left((2n)^3(\deg f + 1)^{6n^2}\right).$$

■

Remarque 2. — Ici, on n'a pas de problème de contrôle de la taille des coefficient, ce qui nous laisse d'avantage de latitude sur le choix d'un algorithme de calcul de la base standard. Si toutefois, on souhaitait majorer le coût des calcul élémentaires en machine, avec par exemple des coefficients entiers ou rationnels, il faudrait procéder comme pour la démonstration du théorème 4 ci-dessus.

§ 3. BASES CANONIQUES DE SOUS-ALGÈBRES

1. Introduction

On introduit ici la notion de base canonique de manière directe. On trouvera à la fin du paragraphe quelques remarques sur le lien avec le formalisme du § 1.

Les *bases standard* sont apparues pour la première fois dans les travaux de HIRONAKA, du moins sous une forme explicite. BUCHBERGER donna ensuite un algorithme de construction et les désigna sous le nom de bases de Groebner. Cette notion a joué depuis un rôle central pour la résolution formelle des systèmes d'équations algébriques. On peut néanmoins en trouver la trace dans des travaux très antérieurs. Déjà en 1920, JANET, cherchant à décrire l'ensemble des monômes de tête d'un idéal introduit des ensembles de générateurs qui évoquent quelque peu les bases standard. Pour caractériser les monômes de tête de l'idéal $[x^p]$, H LEVI utilise déjà (en 1942 !) un ordre admissible et des procédés proches de la réécriture (8).

Ces résultats apparaissent dans leur forme originale de manière assez complexe et technique, précisément parce qu'une notion explicite de base standard faisait défaut pour les formuler.

Les bases canoniques de sous-algèbres ont, semble-t-il, une histoire plus courte. Elles apparaissent pour la première fois dans l'article [KM] de KAPUR et MADLENER qui les ont élaborées en 1988. Indépendamment, ROBBIANO et SWEEDLER introduisaient des objets identiques sous le nom de SAGBI, *Subalgebra Analogs for Groebner Bases of Ideals*. Leurs résultats ont été rédigés dans [RS].

À l'inverse des bases standard, les bases canoniques peuvent être infinies, même pour des sous-algèbre de type fini. Cet inconvénient majeur, qui n'apparaît pas pour les bases standard d'idéaux algébriques a, semble-t-il, contribué à différer la publication de ces travaux.

Quoi qu'il en soit, les bases canoniques offrent souvent un moyen efficace de calcul par rapport aux méthodes utilisant le graphe et les bases standard.

2. Monoïdes et bases standard

Sauf précision explicite, k désignera un corps de caractéristique arbitraire, $k[n]$ l'algèbre des polynômes en n variables sur k $k[x_1, \ldots, x_n]$ et M un monoïde abélien avec une loi additive. Si E est un sous-ensemble de M, Mon*E désignera le sous-monoïde de M engendré par E.*

2.1. Monoïdes abéliens et algèbres de monoïdes

Avant d'en venir aux bases canoniques, il est utile de rappeler explicitement quelques résultats relatifs aux monoïdes, bien qu'ils soient en principe "bien connus". Le lecteur pourra se reporter à [Jo] pour plus de détails. On ne considère ici que des monoïdes abéliens et les monoïdéaux seront donc à la fois des monoïdéaux à gauche et à droite.

On rappelle qu'un monoïdéal de M est un sous-ensemble I de M tel que $x + M \subset I \; \forall x \in I$. Tout monoïde a une structure naturelle d'ensemble partiellement préordonné, ou préposet, définie par $x \leq y$ si $\exists z \; y = x + z$. Cet ordre est compatible avec la structure de monoïde, c'est-à-dire que $x \leq y$ implique $x + z \leq y + z$. Pour tout préposet E, on appelle escalier engendré par une partie F et l'on note $\mathrm{E}(F)$ l'ensemble $\{x \in E | \exists y \in F \; x > y\}$. Pour un monoïde muni de l'ordre canonique, les escaliers coïncident avec les monoïdéaux.

On peut associer à tout monoïde abélien M et à tout anneau R abélien une algèbre de monoïde abélienne $R[M]$ (9). Cette algèbre correspond au R-module des combinaisons

(8) On se reportera à [Lev] et [Ri2 chap. I § 21 p. 16] pour plus de détails.

(9) On trouvera dans [Jo] la notation $A\langle M\rangle$ que je préfère réserver ici à l'algèbre différentielle pour éviter des confusions.

linéaire formelles

$$\sum_{m \in M} c_m . m,$$

avec les c_m presque tous nuls, la multiplication étant telle que $(c.m)(c'.m') = cc'.(m+m')$. Les éléments de la forme $1.m$ seront appelés monômes, et ceux de la forme $c.m$ termes.

L'algèbre des polynômes en n variables $R[n]$ n'est autre que l'algèbre $R[\mathbf{N}^n]$. Si M est un sous-monoïde de $\mathbf{N}^n$, on peut considérer $k[M]$ comme un sous-monoïde de $k[n]$. En général, notant $\mathbf{N}^{(S)}$ le monoïde abélien libre construit engendré par un ensemble S, l'algèbre de polynômes $R[S]$ est l'algèbre de monoïde $R[\mathbf{N}^{(S)}]$. Il y a des relations intimes entre les propriétés des monoïdes et celles de leurs k-algèbres. Par exemple, tout monoïde M de type fini est cohérent pour l'ordre canonique, ce qui signifie que tous ses escaliers, ou monoïdéaux, sont de type fini. Cette propriété implique que $k[M]$ est un anneau noetherien.

La situation est moins agréable, lorsqu'on considère les sous-monoïdes. En effet, $\mathbf{N}^n$ peut admettre des sous-monoïdes de type infini, sauf si $n = 1$. Cela signifie qu'il existe des sous-algèbres non finiment engendrées de $k[n]$, sauf dans le cas en une variable.

Il y a une bijection naturelle entre les ordres admissibles sur les monômes de $k[n]$ et les ordres compatibles de $\mathbf{N}^n$ tels que $x > 0$ $x \neq 0$(voir [Ro1]), qu'on appellera aussi ordres admissibles par extension. Ayant choisi un ordre admissible $\prec$, on peut associer à tout polynôme non-nul $P = c\,x_1^{\alpha_1} \cdots x_n^{\alpha_n} + \cdots$ son multidegré $\operatorname{mdeg} P = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$. Alors, pour tout idéal $\mathcal{I}$ (resp. toute sous-algèbre A) de $k[n]$, l'ensemble mdeg$\mathcal{I}$ (resp. mdeg$A$) est un monoïdéal (resp. sous-monoïde) de $\mathbf{N}^n$.

PROPOSITION 1. — *Tout ordre admissible $\prec$ de $\mathbf{N}^n$ est un bon ordre. En d'autres termes, toute chaîne strictement décroissante*

$$x_0 \succ x_1 \succ \cdots \succ x_k \succ x_{k+1} \succ \cdots$$

est finie.

PREUVE. Voir, par exemple, [Ko2 chap. 0 § 17 lemme 15 p. 49]. ∎

COROLLAIRE 1. — *Tout sous-monoïde M de $\mathbf{N}^n$ admet un unique ensemble minimal de générateurs.*

PREUVE. La proposition implique que le préordre canonique sur M est un bon ordre. On en déduit aisément que l'ensemble G des éléments non nuls de M minimaux pour le préordre canonique forment un ensemble de générateurs. D'autre part, les éléments de G appartiennent à tout ensemble de générateurs, d'où l'unicité. ∎

2.2. Méthode du graphe et algèbres monomiales

On va donner des relations entre les congruences sur un monoïde M et les idéaux binômiaux de $k[M]$. On en déduira une méthode permettant de déterminer un système de générateurs de certaines congruences, et de tester l'appartenance d'un élément à un monoïde.

DÉFINITION 1. — *On appellera idéal binomial de $k[M]$ un idéal engendré par des éléments de la forme $m - m'$, où m et m' sont deux monômes.*

DÉFINITION 2. — *Une congruence sur un monoïde M est une relation d'équivalence C telle que $\forall (x, y, z) \in M^3 \ x \equiv y \Rightarrow x + z \equiv y + z$.*

Il est bien connu que la structure de monoïde sur M induit une unique structure de monoïde sur l'ensemble quotient, telle que l'application canonique de M dans M/C soit un morphisme de monoïde.

PROPOSITION 2. — *Une relation d'équivalence $C \subset M \times M$ est une congruence ssi c'est un sous-monoïde de $M \times M$.*

PREUVE. Voir [Jo 1.4.1 p. 14]. ∎

PROPOSITION 3. — *Soit R un anneau intègre et C une congruence sur le monoïde M, on lui associe l'idéal binomial $\mathcal{I}$ engendré par les éléments de $R[M]$ de la forme $m - m'$, où $(m, m') \in C$. Alors $(m, m') \in C$ ssi $m - m' \in \mathcal{I}$.*

PREUVE. Voir [MM lemmes 1 et 2 p. 311], où une preuve est donnée pour $\mathbf{Z}$ qui s'étend aisément à n'importe quel anneau intègre. ∎

En particulier, il est utile en pratique de considérer $\mathbf{Z}/2\mathbf{Z}$.

On aura besoin de la proposition suivante qui permet de construire une sorte de "base standard" pour une congruence, en construisant une base standard de l'idéal associé.

PROPOSITION 4. — *Si C est une congruence sur $\mathbf{N}^n$ et $\mathcal{I}$ l'idéal qui lui est associé par la construction de la proposition précédente, alors pour tout ordre total admissible sur les monômes de $k[n]$, les polynômes dans la base standard réduite G de $\mathcal{I}$ sont des différences de monômes, et l'ensemble $\{(m, m') | m - m' \in \mathcal{G}\}$ engendre la congruence.*

PREUVE. On se convainc aisément que les polynômes de G sont des différences de monômes, car $\mathcal{I}$ est engendré par des polynômes de ce type, ce qui implique que les S-polynômes entre les générateurs le sont aussi.

La dernière partie résulte de la preuve de [Jo cor. 1.6.6.2 p. 34]. ∎

COROLLAIRE 1 (Théorème de Redei). — *Toute congruence dans $\mathbf{N}^n$ est finiement engendrée en tant que congruence, et en tant que monoïde.*

PREUVE. La première partie est immédiate d'après la proposition. La seconde résulte du fait qu'une congruence sur un monoïde M engendrée par une partie $E \in M \times M$ est engendré comme monoïde par E, $\sigma(E) = \{(y, x) | (x, y) \in E\}$ et $D = \{(x, x) | x \in M\}$: $\sigma(E)$ est fini, et D est isomorphe comme monoïde à $\mathbf{N}^n$, donc de type fini. ∎

COROLLAIRE 2. — *Soit ϕ: $\mathbf{N}^n \mapsto \mathbf{N}^m$ et ψ: $\mathbf{N}^\ell \mapsto \mathbf{N}^m$ deux morphismes de monoïdes et M le sous-ensemble de $\mathbf{N}^n \times \mathbf{N}^\ell$ défini par $M = \{(x, y) | \phi(x) = \psi(y)\}$, alors M est de type fini.*

PREUVE. Il suffit d'identifier l'élément (x, y) de M avec l'élément $((x, 0), (0, y)$de $(\mathbf{N}^n \times \mathbf{N}^\ell) \times (\mathbf{N}^n \times \mathbf{N}^\ell)$. M engendre une congruence C de $\mathbf{N}^n \times \mathbf{N}^\ell$, qui est de type fini. Ceci implique qu'une partie finie de M engendre C comme congruence et M comme monoïde. ∎

Remarques. — 1) On sait (voir [Ro1]) que tout ordre total admissible sur $\mathbf{N}^n$ est induit par un morphisme de monoïde ϕ: $\mathbf{N}^n \mapsto \mathbf{R}^m$, où $\mathbf{R}$ est ordonné par l'ordre lexicographique pur. De tels ordre étaient déjà utilisés par RIQUIER et JANET dans leurs travaux en algèbre différentielle. ROBBIANO a donné dans son article une description complète de ces ordres et montré qu'on pouvait prendre $m \leq n$.

2) Si l'on considère un sous ensemble S de $k[n]$, et le morphisme

$$\begin{array}{llll}\psi\colon & k[\mathbf{N}^{(S)}] & \mapsto & k[n] \\ & R & \mapsto & R(S),\end{array}$$

tout préordre total admissible de sur les monômes de $k[n]$ induit un préordre total admissible sur les monômes de $k[\mathbf{N}^{(s)}]$, et donc une graduation.

PROPOSITION 5. — *Soit M le sous-monoïde de $\mathbf{N}^n$ engendré par l'ensemble fini $\{\alpha_i\,; i \in [1,m]\}$. On définit sur $\mathbf{N}^n \times \mathbf{N}^m$ une congruence associée au morphisme de monoïde défini par $\phi(e_i) = \alpha_i$, où e_i désigne le i ème générateur élémentaire de $\mathbf{N}^m$, et $\phi(x) = x$ pour tout x dans $\mathbf{N}^n$. On note également ϕ le morphisme de k-algèbres associé. Soit $\prec$ un préordre ordre total admissible sur $\mathbf{N}^n$, on peut l'étendre en un préordre admissible sur $\mathbf{N}^n \times \mathbf{N}^m$, en utilisant le morphisme ϕ, et le compléter en un ordre total admissible $\ll$ en raffinant par un ordre total d'élimination pour les n premières variables. Alors la base standard G de l'idéal $\mathcal{I} = (x^{\alpha_i} - y_i)_{k[x_1,\ldots,x_n,y_1,\ldots,y_m]}$ est telle que :*

a) $\beta \in \mathbf{N}^n$ appartient à M ssi $x_\beta \xrightarrow{G^\star} y^\gamma$,

b) $G \cap k[y] = \{y^{\beta_i} - y^{\gamma_i}\,; i \in [1,s]\}$, et les couples (β_i, γ_i) engendrent la congruence induite par ϕ sur $\mathbf{N}^m$.

PREUVE. On commence par remarquer que l'idéal $\mathcal{I}$ est homogène pour la graduation induite par $\prec$. Ceci implique que $G \cap k[y]$ engendre $\mathcal{I} \cap k[y]$ puisque $\ll$ est obtenu en raffinant par un ordre d'élimination. D'autre part, $\mathcal{I}$ est binomial, donc G est constitué de différences de monômes. Utilisant alors la proposition 4, on en déduit que les couples (β_i, γ_i) engendrent la congruence induite sur $\mathbf{N}^m$.

Enfin, β appartient à M ssi x^β appartient à la sous-algèbre $k[M]$ de $k[\mathbf{N}^n]$, donc utilisant le th. 2.1.1 p. 49, ceci est équivalent à $x_\beta \xrightarrow{G^\star} y^\gamma$.

Remarque 3. — Comme l'idéal $\mathcal{I}$ est homogène, pour tester l'appartenance d'un élément β à M, il suffit de calculer la base standard de $\mathcal{I}$ jusqu'à un ordre au plus égal à celui de β, selon la graduation associée à $\prec$.

La suite de ce paragraphe reprend le corps de l'article [O2], que des contraintes de temps m'ont empêché de traduire. Je prie les lecteurs de bien vouloir m'en excuser.

3. Canonical Bases

We will denote by $k[n]$ the algebra of polynomials in n variables $x_1, \ldots, x_n$. We give ourselves an admissible ordering $\prec$ on monomials of $k[n]$. The leading coefficient of a polynomial P will be denoted by $\mathrm{lc}P$ and the leading primitive monomial of P by $\mathrm{m}P$. A will denote a k-subalgebra of $k[n]$. To avoid useless complications, we will suppose all polynomials to be monic, if not stated otherwise. It will be easy to think of the necessary modifications if it is not the case.

3.1. Definition

DEFINITION 3. — *Let A be a k-subalgebra of $k[n]$ and E a subset of A, we denote by* $\mathrm{Mon}\, E$ *the submonoid of* $\mathbf{N}^n$ *generated by* $\{\mathrm{mdeg}P | P \in A\}$. *A subset E of A is said to be a canonical basis of A if* $\mathrm{Mon}E = \mathrm{Mon}A$.

Obviously, we have a similar definition for standard bases by replacing k-subalgebra by ideal and submonoid by e-set—or monoideal.

An admissible ordering being given, we can associate to any subset of a k-subalgebra a reduction relation, in the following way.

DEFINITION 4. — *Let Q, and Q' be two polynomials of $k[n]$ and C a subset of $k[n]$, then we say that Q is reduced to Q' by C if* $\mathrm{mdeg}Q \in \mathrm{Mon}C$ *and*

$$Q' = Q - \prod_{i=1}^{k} R_i^{\alpha_i},$$

where the α_i and R_i are integers and elements of C such that $\mathrm{mdeg}Q = \sum_{i=1}^{k} \alpha_i \mathrm{mdeg}R_i$. *This relation will be written*

$$Q \xrightarrow{P} Q'.$$

We will denote by $\xrightarrow{C^\star}$ *the inductive limit of the relation* $\xrightarrow{C}$.

We say that P is reduced with respect to C if there is no Q such that $P \xrightarrow{C} Q$, *and that P is strongly reduced if P is reduced and the reductum of P is strongly reduced, which means that no monomial of P belongs to* $\mathrm{Mon}C$.

DEFINITION 5. — *We say that C is a reduced canonical basis of A if C is a canonical basis, the polynomials in C are monic and each polynomial $P \in C$ is strongly reduced with respect to $C \setminus \{P\}$.*

As k is a field, any k-subalgebra A admits a unique reduced canonical basis, which is finite iff A admits a finite canonical basis. We will refer to the reduced canonical basis as *the* canonical basis of A.

Lemma 1. — *If P belongs to a k-subalgebra A of $k[n]$ and if C is a subset of A, then any polynomial Q such that* $P \xrightarrow{C^\star} Q$ *belongs to A.* ∎

Lemma 2. — *Any chain of reduction*

$$Q_0 \xrightarrow{C} Q_1 \ldots Q_{k-1} \xrightarrow{C} Q_k \xrightarrow{C} \ldots$$

has to be finite.

PROOF. This is a simple consequence of prop 2.1.1 p. 55. ∎

DEFINITION 6. — *If C is a subset of $k[n]$ we can extend any admissible ordering $\prec$ on monomials of $k[n]$ to a preordering on* $k[\mathbf{N}^{(C)} \times \mathbf{N}^n]$ *by setting* $m \prec m' \Leftrightarrow m(C,x) \prec m'(C,x)$. *That preordering will be used each time we will deal with polynomials in* $k[\mathbf{N}^{(C)} \times \mathbf{N}^n]$ *or* $k[\mathbf{N}^{(C)}]$. *The multidegree of a polynomial R will be then the maximal multidegree of $m(C)$, for all monomials m of R.*

Lemma 3. — *If $P \xrightarrow{C^\star} 0$, then there exists a polynomial $R \in [\mathbf{N}^{(C)}]$, of multidegree not greater than P, such that $R(C) = P$.*

PROOF. We can build R by reducing P, each step of reduction giving a monomial. The monomials appear then in strictly decreasing order according to $\prec$. ∎

The following notion is an analog of syzygies in the case of standard bases.

DEFINITION 7. — *Let C be a subset of $k[n]$, $\{P_1, \ldots, P_\ell\}$ and $\{Q_1, \ldots, Q_m\}$ two finite subsets of C, whose elements are all different, let M be the submonoid of $\mathbf{N}^\ell \times \mathbf{N}^m$ whose elements $((\alpha_1, \ldots, \alpha_\ell), (\beta_1, \ldots, \beta_m))$ satisfy*

$$\sum_{i=1}^{\ell} \alpha_i \mathrm{mdeg} P_i = \sum_{i=1}^{m} \beta_i \mathrm{mdeg} Q_i.$$

Then, we call a superposition between elements of C a 4-uple $((P_1, \ldots, P_\ell), (Q_1, \ldots, Q_m), \alpha, \beta)$, such that (α, β) belongs to the minimal set of generators of M.

The polynomial

$$\prod_{i=1}^{\ell} P_i^{\alpha_i} - \prod_{i=1}^{m} Q_i^{\beta_i}$$

is called the S-polynomial associated to the superposition. The multidegree of the superposition is the common multidegree of both products in the formula above.

Remark 1. — With the same notations, the 2-uples of exponents $((\alpha_P), (\beta_Q))$ associated to all superpositions between elements of C, generate the congruence defined by

$$\sum_{P \in C} \alpha_P \mathrm{mdeg} P = \sum_{Q \in C} \beta_P \mathrm{mdeg} Q.$$

In this case, minimal sets of generators do not exist, but if C is finite, the construction of prop. 2.2.5 p. 57. provide a finite set of superposition, generating the congruence, which is in general smaller than the set of all superpositions.

DEFINITION 8. — *If $\mathcal{S}$ is a set of superpositions generating the congruence defined above, it is said to be a generating set of superpositions. It is said to be confluent if all the corresponding S-polynomials are reduced to 0 by C.*

Lemma 4. — *If C is a subset of $k[n]$, m and m' two monomials of $k[\mathbf{N}^{(C)}]$ such that $m(C)$ and $m'(C)$ have the same leading monomial and $\mathcal{S}$ a generating set of superpositions, then there exist ℓ monomials M_i of $k[\mathbf{N}^{(C)}]$ and S-polynomials R_i associated to superpositions of $\mathcal{S}$ such that*

$$m(C) - m'(C) = \sum_{i=1}^{\ell} M_i(C) R_i.$$

∎

We have then a fundamental theorem, which also has an analog in the case of standard bases.

THEOREM 1. — *Let A be a k-subalgebra of $k[n]$ and C a subset of A, then the three following propositions are equivalent:*

A) C is a canonical basis,

B) $\forall P \in A \;\; P \xrightarrow{C^*} 0$,

C) C generates A and there exists a generating confluent set $\mathcal{S}$ of superpositions between elements of C.

PROOF. A) $\Rightarrow$ B) For any element P of A, mdeg$P$ is in Mon$C$ so that P needs to be reduced by C if P is not 0. By lemmas 1 and 2, $P \xrightarrow{C^*} 0$.

B) $\Rightarrow$ C) As any polynomial in A is reduced to 0, it is obviously the case of any S-polynomial. This also implies that C generates A.

C) $\Rightarrow$ A) That will be the consequence of a more precise result.

PROPOSITION 6. — *If $P = T(C)$ is a polynomial in A and if all superpositions between elements of C of multidegree not greater than the multidegree of T are reduced to 0 by C, then P is reduced to 0 by C.*

PROOF. We recall that we have extended $\prec$ to an ordering on monomials of $k[\mathbf{N}^{(C)}]$. We suppose the result is false and search a contradiction. Let us consider the non reducible $P = R(C)$ such that R is minimal according to $\prec$, we have $R \preceq T$. Then we can choose some P among them such that R has minimal number of monomials.

Let m be a maximal monomial of R, $m(C)$ is obviously reducible, and $R(C) - m(C)$ is reducible too, for its maximal monomials are not greater than m and $R - m$ has smaller number of monomials than R. $m(C)$ and $R(C) - m(C)$ have the same leading monomial and opposite leading coefficients, if not P would be reducible. Then $R(C) - m(C) \xrightarrow{C} Q(C)$, with $Q(C)$ reducible so that Q is smaller than $R - m$ according to lemma 3. Now $R(C) - m(C)$ is equal to $m'(C) + Q(C)$ where m' is a monomial greater than Q. $m(C)$ and $m'(C)$ have obviously opposite leading monomials and by lemma 4, $m(C) - m'(C)$ is of the form $\sum m_i S_i$, where the S_i are S-polynomials associated to superpositions in C and the $m_i S_i$ are smaller than R. We can then use the hypothesis on S-polynomials and apply again lemma 3 on each $m_i S_i$. So $m(C) + m'(C) = Q'(C)$ with Q' smaller than R.

The conclusion of this construction is that $P = Q(C) + Q'(C)$ and $Q + Q'$ is smaller than R, a contradiction. ∎

Remark 2. — We have no need in this proof to suppose that A is of finite type, nor that C is finite. Of course, we shall have to restrict ourselves to that case for effective applications.

3.2. Completion Procedure. Implementation

Using prop 2.2.5 p. 57, we can solve the membership problem for Mon$C$, and it is then easy to build a reduction procedure. The same standard basis construction will give a generating set of superpositions, so that the construction of superpositions is also effective (see also [Hu]).

DEFINITION 9. — *We say that a completion procedure is fair if all S-polynomials which are not discarded using some criteria have to be considered and reduced during the computation.*

For example, if we sort S-polynomials according to the multidegree of corresponding superposition the procedure is fair iff the ordering is archimedean. We have then the following result.

The algorithm is described using the syntax of Scratchpad II (cf. [Scr]).

THEOREM 2. — *Let A be $k[P_1, \ldots, P_m]$, then if A admits a finite canonical basis, any fair procedure of the following form will stop and return a canonical basis:*

$C := [P_1, \ldots, P_m]$
$LS := [\,]$
until $LS = [\,]$ repeat
  $LS :=$ *List-of-S-polynomials-not-considered-yet*(C)
  if $LS = [\,]$ then leave
  $Sp :=$ *Choose*(LS) ; $LS := LS - [Sp]$
  if *Red*$(Sp) \neq 0$ then $C :=$ *cons*(*Red*$(Sp), C)$
  output(C)
C

If A admits no finite standard basis, the sets of polynomials C_i, returned at each loop are such that $\bigcup_{i=1}^{\infty} C_i$ is a standard basis.

PROOF. See [KM]. ∎

Remark 3. — We did not implement exactly a procedure of that type. Superpositions are determined, using a standard computation as described in 1.2.8. Each time a new element corresponding to a superposition is appended to the standard basis, its computation is suspended after returning the superposition to the canonical basis process. It computes the S-polynomial, reduces it, updates the list C as above and call the standard basis algorithm again. In this way, not all superpositions are found, but we still secure a generating set, which is enough, and better for efficiency. If a superposition corresponds to the reduction of a polynomial in C, we can discard it.

This algorithm is fair iff $\prec$ is archimedean. This is the case for the degree ordering, implemented in Scratchpad II. It would have been too complicated and inefficient to use the standard basis algorithm of the public system (implemented by Gebauer and Moeller), so that we have rewritten it in the case of binomial ideals and made it incremental. We use $\prec$, refined by the inverse lexicographical ordering on variables, sorted by "order of appearance". Indeed, for each element appended to C, a new variable appear in the standard basis computation. With such an ordering, we will never have to consider superpositions involving a polynomial which has been removed.

Two packages have been implemented, STANDMON computes standard bases for binomial ideals, monomials with suitable ordering been implemented in the domain MOFAM. The last package, BASECAN implements the canonical bases process.

Remarks. — 4) During the standard basis computation, some superpositions may be found, coming from the reduction of a syzygy between two superpositions—as in prop. 2.2.5 p. 57, superpositions are identified with binomials. In such a case, this superposition needs not to be considered, for it is generated by superpositions already treated and reduced. It seems that with the chosen ordering such a situation never occurs.

5) Reducing to a generating set of superpositions is the canonical bases analog of the criterion of MOELLER allowing to reduced the set of syzygies to a generating set of the module of relations between leading monomials (see [Mol]).

4. Relations with Standard Bases

We will consider here a k-subalgebra A of $k[n]$ with a finite canonical basis C, according $\prec$. M will denote the submonoid Mon$A$.

4.1. A Generalization of Standard Bases

The generalized standard bases presented here are special cases of those described by SWEEDLER in [Sw] and ROBBIANO in [Ro2]. The connection made with canonical bases allows simpler definitions, and a more effective presentation. Moreover, canonical bases could be extended too, in the same way as SWEEDLER did for standard bases.

We first remark that if A is of finite type—it is obviously the case if A admits a finite canonical basis—then A is noetherian. So we may hope to generalize standard bases to A without much trouble. We will see it is indeed the case.

DEFINITION 10. — *Let I be an ideal of A, M the submonoid* Mon$A$ *and E the e-set $\{\mathrm{mdeg}P | P \in I\}$ of M. Then we say that a subset G of I is a standard basis of I if the set $\{\mathrm{mdeg}P | P \in G\}$ generates E as an M-monoideal.*

Remark 1. — We have to notice that we must use the same ordering to define the canonical basis and the standard basis. In the case of $k[n]$, we do not have such a trouble for $\{x_1, \ldots, x_n\}$ is a canonical basis for all orderings. As shown in [RS], other algebras share this property, for example the elementary symmetrical polynomials form a standard basis of the subalgebra of symmetrical polynomials, for all orderings.

PROPOSITION 7. — *All ideals of a k-subalgebra A admitting a finite canonical basis, admit a finite standard basis.*

PROOF. With the same notations as in the definition, M is of finite type so that it is coherent and E is of finite type. ■

We will now generalize the notion of syzygy.

DEFINITION 11. — *Let $S = \{R_1, \ldots, R_q\}$ be a finite subset of a A, which admits a finite canonical basis $C = \{P_1, \ldots, P_\ell\}$, Q and R two elements of S, and E the set of 2-uple of monomials $(m, m') \in k[\ell] \times k[\ell]$ such that*

$$\mathrm{mdeg}(m(P)Q) = \mathrm{mdeg}(m'(P)R).$$

Denoting by M the submodule generated by E, we call syzygy between Q and R a 4-uple (R, S, m, m'), such that (m, m') belongs to the minimal subset of E which generates M.
■

Remark 2. — Such minimal elements are in finite number and we can again restrict ourselves to a generating set of syzygies, obtained in the following way. We consider the polynomial algebra $k[w, x, u, y]$, with 1 variable w, n variables x, q variables u associated to the polynomials R, and ℓ variables y associated to the polynomials P. We define weights on variables such that the weight of w and the u is 1, and the weight of the other variables 0. The binomial ideal $(\mathrm{m}P_i - y_i, w\mathrm{m}R_j - u_j)$ of $k[u, x, w, y]$, is homogeneous for this weight—this is why we need the extra variable w. Then, we compute the standard basis of this ideal up to weight 1, for an ordering which respects the total weight, eliminates w and the x and then the u.

The elements of this basis of weight 1, whose leading monomial depends only of the variables u and y are of the form $\prod y^{\alpha_i} u_j - \prod y^{\beta_i u_{j'}}$. They are associated to a set of syzygies, generating the module of relations between leading monomials. As pointed out by P. Conti and C. Traverso in [CT], an efficient algorithm for standard bases of modules can be derived from an algorithm for ideals if we forget syzygies of weight 2 and more.

The considerations of remarks 3.2.4–5. p. 61–62 also apply in this case.

Remark 3. — We have seen that in the case of canonical bases, superpositions involve in general more than two polynomials. Here, syzygies involve only two polynomials, but there can be more than just one syzygy between two given polynomials (see [Sw]).

We can define a notion of reduction with respect to a subset G of A in an obvious way and we get the usual theorem.

Theorem 3. — *If A is a k-subalgebra of $k[n]$, I an ideal of A and G a subset of I, then the following properties are equivalent:*

A) G is a standard basis of I,

B) all elements of I are reduced to 0 by G,

C) G generates I and there exists a generating confluent set of syzygies between elements of G.

proof. We can adapt the proof of th. 3.2.2 p. 61, or any proof for "usual" standard bases (see [Bu2]). ∎

Again, we will have a completion procedure, relying on successive reductions of S-polynomials.

4.2. Ideal of Relations

Definition 12. — *Let A be a k-subalgebra of $k[n]$ admitting a finite canonical basis $C = \{P_1, \ldots, P_m\}$, then we can define an ideal of relations between polynomials of C by $I = \{R \in k[m] | R(P) = 0\}$.*

Definition 13. — *Let S be a superposition between elements of a finite canonical basis $C = \{f_1, \ldots, f_m\}$, P the S-polynomial associated to S. Reducing $P(f)$ to zero by C, we secure a polynomial $R(f)$, of smaller multidegree than P, such that $P - R \in I$. We denote $P - R$ by $R(S)$.*

THEOREM 4. — *With the same notations, if we consider the whole generating set of superpositions G determined by a standard basis computation, using some total ordering $\ll$ compatible with $\prec$ as described in cor. 1.2.7, then the set of polynomials $R(G)$ associated by the previous construction form a standard basis of the ideal of relations I according to $\ll$.*

PROOF. It is easily seen using prop. 2.2.5 p. 57 and lem. 3.1.4 p. 59 that all polynomials in I are reduced to 0 by $R(G)$. ∎

5. Finiteness Conditions

5.1. Examples

We will begin by two examples of ROBBIANO, which show that the canonical basis of a finitely generated k-subalgebra may be infinite.

Example 1. — Let $A = k[x, xy - x^2, xy^2] \in k[x, y]$. If k is of characteristic 0 and if we consider some ordering with $x > y$, then the reduced canonical basis of A is is

$$\{x, xy - y^2, xy^2, xy^3 - \frac{1}{2}y^4, xy^4, xy^5 - \frac{1}{3}y^6, \ldots\},$$

so that A admits no finite canonical basis. If we consider some ordering with $y > x$, then the canonical basis is finite.

If k is of positive characteristic p, then A admits a finite canonical basis for all orders, for then $y^{2p} \in A$.

It takes 11 s. to compute the standard basis with $x > y$ up to degree 7, using Scratchpad II. Only 2 S-polynomials are reduced to 0 during this computation. As the degree increases, more and more unuseful and undetected superpositions are considered, coming from the particular structure of the algebra; $d - 3$ well chosen superpositions would be enough to go up to degree d.

Example 2. — Let A be $k[x + y, xy, xy^2]$, where k is an arbitrary field, then the canonical basis of A for some ordering with $x > y$ is

$$\{x + y, xy, xy^2, xy^3, xy^4, \ldots\}.$$

If we take $y > x$ then the canonical basis is also infinite by symmetry.

Remark 1. — We can remark on those two examples that A is not integrally closed and that its integral closure is $k[x, y]$, which has a finite canonical basis.

In example 1, the extension $A[y^2]$ is an integral extension of A with finite canonical basis. Indeed, $y^2 = xy^2/x$ is in the integral closure, so that $I = xA$ is both a A ideal and a $A[y^2]$ ideal. Now, if we want to test that a polynomial P is in A, this can be done by computing a generalized standard basis for I in $A[y^2]$ and then test if xP belongs to I. In example 2, we can take $A[y] = k[x, y]$, and remarking that $y = xy^2/xy$ is in the integral closure, consider the ideal $xy\,A = xy\,A[y]$.

This method generalizes each time we know (by its generators) an integral extension B=$A[P_i/Q_i]$ of A in its fraction field, with finite canonical basis. The ideal $I = (\prod Q_i^{a_i-1})\,A$, where a_i is the degree of a monic polynomial $R_i \in A[z]$ such that $A_i(P_i/Q_i) = 0$, is equal to $(\prod\, Q_i^{a_i-1})\,A[P_i/Q_i]$. This allows to reduce the membership problem for A to the membership problem for a the B ideal I, generated by a single element.

We can easily apply to those two examples the method of Shannon and Sweedler, but we can give some example where this method fails whereas the canonical basis method have a pretty good complexity.

Example 3. — If we consider the k-subalgebra A of $k[n]$ generated by the n polynomials

$$\begin{aligned} P_1 &= x_1 + \cdots + x_n \\ P_2 &= x_1x_2 + x_2x_3 + \cdots + x_nx_1 \\ &\ \vdots \\ P_n &= x_1x_2\cdots x_n, \end{aligned}$$

the standard basis of Shannon and Sweedler's method cannot be computed with the program Macaulay of BAYER and STILLMAN, already for $n = 7$. But the canonical basis of A for the degree ordering is $\{P_1, \ldots, P_n\}$. Indeed, there is no superposition between those polynomials, for their multidegrees are linearly independent. We can remark that the computation of a canonical basis for the ideal $(P_1, \ldots, P_{n-1}, P_n - 1)$ of $k[n]$ is itself a difficult problem, known as the Arnborg–Davenport problem. For the best of our knowledge it has been done only up to $n \leq 7$, using Macaulay, and $n = 8$ using the program of J. C. FAUGÈRE. It takes more than a week on ALLIANT FX40.

We could give many other examples of this kind, e.g. the polynomials of the Mayr–Meyer examples ([MM]), form a canonical basis for some ordering.

5.2. A Conjecture and Related Results

We have stated in [O2] the following conjecture, to which rem. 5.1.1. p. 64 gives a particular interest.

CONJECTURE. *If A is a finitely generated integrally closed k-subalgebra of $k[n]$, then its canonical basis for any admissible ordering is finite.*

Remark 2. — The hypothesis that A is finitely generated is essential, for there exist integrally closed k-subalgebra of infinite type (consider for example $k[x, xy, xy^2, \ldots] \subset k[x, y]$).

We will give some partial results relating the standard basis of A and that of its integral closure $\overline{A}$.

DEFINITION 14. — *Let A be any k-subalgebra of $k[n]$, we call cone of A, the convex cone $\mathcal{C}A$ generated in $\mathbf{R}_+^n$ by* $\mathrm{Mon}A \in \mathbf{N}^n$, *with vertex at the origin.*

Lemma 5. — *If $P \in k[n]$ belongs to the integral closure $\overline{A}$ of A, then* mdeg$P \in \overline{\mathcal{C}A}$, *which stands for the topological closure of* $\mathcal{C}A$.

PROOF. P belongs to $\overline{A}$ so that $P = R/Q$ with $R \in A$ and $Q \in A$, and P satisfies some polynomial equation $P^k + a_1 P^{k-1} + \cdots + a_k = 0$ where the a_i belong to A. Now, multiplying this equation by Q^k, we get $R^k + a_1 Q R^{k-1} + \cdots + a_k Q^k = 0$, so that R^{k+1}/Q belongs to A. We can now prove by induction that $R^k P^i = R^{k+i}/Q^i$ belongs to A for all positive integer i. The mutidegree of $R^k P^i$ is $k\mathrm{mdeg}R + i\mathrm{mdeg}P$, hence the wanted result. ∎

THEOREM 5. — *Let A be any k-subalgebra of $k[n]$, then*

$$\mathcal{C}A \subset \mathcal{C}\overline{A} \subset \overline{\mathcal{C}A}.$$

PROOF. The first inclusion is obvious and the second is a mere consequence of the lemma. ∎

Remark 3. — Our conjecture would imply that if A is finitely generated, $\mathcal{C}\overline{A} = \overline{\mathcal{C}A}$, for the canonical basis would be finite, so that its cone would be closed and generated by a finite number of points with integral coefficients. Of this, we would deduce that $\mathcal{C}\overline{A}$ is generated by a finite number of integral points for any k-subalgebra. We will see that this result can be proved for graded k-algebras of dimension 2.

5.3. Special Results for 2-dimensional Graded k-Algebras

We will first introduce some results, valid in general case.

PROPOSITION 8. — *Let $A = k[P_1, \ldots, P_n]$ be a finitely generated graded k-subalgebra of $k[n]$ of dimension μ, $I \in k[m]$ be the ideal of relations between polynomials P_i, $\Delta =$ $\mathrm{lcm}(\mathrm{deg}P_i)$, $\delta = \mathrm{gcd}(\mathrm{deg}P_i)$, then if we denote by $H(d)$ the number of elements of degree d in* Mon$A$, *there exist polynomials $R_i \in \mathbf{Q}[x]$ of common degree equal to $\mu - 1$, such that*

$$H(j\Delta + i\delta) = R_i(j),$$

for j great enough. Furthermore $H(j\delta + k) = 0$ for $0 < k < \delta$.

PROOF. The last part is obvious. Now, if we define a degree $\deg_p$ in $k[y_1, \ldots, y_m]$ by $\deg_p(y_i) = \deg P_i$, we can remark that the number of elements of degree $\deg_p = d$ in $k[y_1, \ldots, y_m]$ satisfies the wanted property. The ideal of relations I is obviously $\deg_p$-homogeneous. This implies our result, for we have a finite free resolution of $A = k[m]/I$, which preserves the graduation $\deg_p$. ∎

COROLLARY 1. — *If A is a finitely generated k-algebra of dimension μ and $h(d)$ the number of points of degree less or equal to d in* Mon$A$, *then there exists some polynomial $R \in \mathbf{Q}[x]$ of degree μ such that $h(d) \geq R(d)$.* ∎

DEFINITION 15. — *Let A be a k-subalgebra, we call dimension of $\mathcal{C}A$, the maximal number of linearly independent points in $\mathcal{C}A$.*

PROPOSITION 9. — *If A is a finitely generated k-subalgebra, the dimension of A is equal to the dimension of $\mathcal{C}A$.*

PROOF. The dimension of $\mathcal{C}A$ is the maximal number ℓ of linearly independent points in Mon$A$. If $P_1, \ldots, P_\ell$ are polynomials of A such that their multidegrees are linearly independent, then $k[P]$ is isomorphical to $k[\ell]$, so that $\dim A \geq \ell$. We also have $\dim A \leq \ell$ by prop. 8 cor. 1 p. 66, hence the result. ∎

We will need the following simple lemma about submonoids of $\mathbf{N}^n$.

Lemma 6. — *If M is a submonoid of $\mathbf{N}^n$ and $p_1, \ldots, p_m$ points in $\mathcal{C}M$, then if we denote by G the subgroup of $\mathbf{Z}^n$ generated by M, there exist a point $q \in \mathcal{C}M$ such that the cone $\mathcal{C}'$ of vertex q generated by the points $p_i + q$ satisfies $M \cap \mathcal{C}' = G \cap \mathcal{C}'$.* ∎

PROPOSITION 10. — *If A is a 2-dimensional graded finitely generated k-subalgebra of $k[n]$, then for any ordering $\prec$, $\overline{\mathcal{C}A}$ is generated by 2 points in $\mathbf{N}^n$.*

PROOF. We will prove this result in $k[x, y]$, but the argument also applies in $k[n]$. We can remark that at most 2 canonical bases exist for A, one for orderings such that $x > y$ the other for $y > x$. We can consider only one of these cases, say $x > y$. Let $P_1, \ldots, P_m$ be homogeneous generators of A, $(\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m)$ their multidegrees, we choose P_j such that α_j/β_j is maximal—we consider it is the case if $\beta_j = 0$. It is easily seen that the S-polynomials coming from a superposition between the P_i have smaller slope than P_j. This implies that $p = (\alpha_j, \beta_j)$ generates the right border of $\mathcal{C}A$.

If the left border of $\mathcal{C}A$ is vertical, we have our result, if not we have to prove that its slope σ is rational. We denote by D the lcm of the degrees of P_i. By lemma 6, for any point $p' = (1, \sigma - \varepsilon) \in \mathcal{C}A$, the number $\mu(aD)$ of points of degree aD in $\mathcal{C}\{p, p'\} \cap \mathrm{Mon}A$ is asymptotically equivalent to the number of points in $G \cap \mathcal{C}'$. We denote by $\nu(aD)$ the number of points of degree aD in $\mathcal{C}\{p, (1, 1+\varepsilon)\} \cap G$. We can remark then that the number of points of degree aD in $G \cap \mathbf{R}^n_+$ is equivalent to aD/r for some integer r, so that

$$\frac{aD}{r}\Big(\frac{\sigma+\varepsilon}{1+\sigma+\varepsilon} - \frac{\beta}{\alpha+\beta}\Big) \sim \nu(aD) \geq H(aD) \geq \mu(aD) \sim \frac{aD}{r}\Big(\frac{\sigma-\varepsilon}{1+\sigma-\varepsilon} - \frac{\beta}{\alpha+\beta}\Big).$$

Now, by prop. 1, σ must be rational. ∎

This result is not sufficient to conclude, but it is still encouraging to prove—even in a special case—a consequence of the conjecture. Assume we can prove that the topological closure of the cone is finitely generated for any finitely generated algebra. An idea to go ahead would be to prove then that for any generator of the cone $a \in \mathbf{N}^n$, one of the two following propositions is true:

i) there exists a polynomial in A, which multidegree is a multiple of a,

ii) there exist a polynomial $P \in k[x_1, \ldots, x_n]$, with multidegree a multiple of a, and a polynomial $R \in A$ such that $\forall p \in \mathbf{N}\ RP^p \in A$, which implies $P \in \overline{A}$.

6. Application to Morphisms of $k[n]$

6.1. Complexity

If we consider an endomorphism of $k[n]$ defined by polynomials $f_1, \ldots, f_n$, it is an automorphism iff $k[f] = k[n]$, so that is can be tested using canonical bases. But, we need to secure a bound in order to stop the computation if $k[P]$ has an infinite canonical basis. That will be a consequence of the theorem proved by Gabber (th. II.2.2.3 p. 28).

We recall f being an endomorphism of $k[n]$ defined by polynomials f_i, the degree of f is the maximum degree of the f_i. Then, if $f \in \mathbf{Aut}_k k[n]$ is of degree d, the degree of f^{-1} is bounded by d^{n-1}.

Theorem 6. — *If $A = k[f_1, \ldots, f_n] = k[n]$ and the maximal degree of polynomials f_i is d, then the canonical basis of A with respect to the degree ordering is $\{x_1, \ldots, x_n\}$ and may be computed by considering only superpositions of degree less or equal to d^n.*

proof. The first part is obvious, and the second is a simple consequence of prop. 3.1.6 p. 60, using the theorem of Gabber. ∎

Of that result, we can deduce a bound on the complexity of the canonical basis computation. It will be of the same order as the bound we can obtain for Shannon and Sweedler's method [(10)], but yet smaller. Indeed the computation of a canonical or standard basis may be considered as a linear algebra problem, once we have secured a bound on the degree of superpositions or syzygies. For the ideal of the graph the bound d^n has been proved in [O1]. Using canonical bases, we have to solve a system of system of $O(d^{n^2})$ equations in $O(d^{n(n-1)})$ variables; for the other method a system of $O(2nd^{2n^2})$ equations in $O(d^{2n^2})$ variables. To be more precise, we proceed with canonical bases as we did in § 2 n° 4, but we do not even need to make polynomials homogeneous. This time the columns are power products of the generating polynomials, whose degree is bounded by d^n, represented in the basis of monomials. Computing a canonical basis reduces again to perform a triangulation of the matrix. Of this, we easily deduce a bound polynomial in d^{n^2} for both methods.

Theorem 7. — *Under the hypotheses of the last theorem, we can test whether A is equal to $k[n]$ with a complexity bounded by*

$$O(d^{3n^2}),$$

in term of elementary operations on the ground field k. ∎

Remark 1. — If we consider the automorphism f of $k[n]$ defined by polynomials $x_1, x_2 + x_1^d, \ldots, x_n + x_{n-1}^d$, then $\deg f^{-1} = d^{n-1}$. This shows that our bound is sharp, and that we will have to climb up to degree d^{n-1} at least using Shannon and Sweedler's method. But the canonical basis of $k[f]$ may be computed in degree d at most. We can obviously build examples where the canonical basis requires to consider superpositions of degree greater than d, but it seems difficult to reach d^n.

---

(10) In this special case the method has been introduced earlier by A. van den Essen in [E].

6.2. Tame Automorphism

We will now consider tame automorphisms of $k[n]$.

DEFINITION 16. — *We say that an automorphism of $k[n]$ is tame if it is in the subgroup generated by elementary automorphisms which are:*

A) the automorphisms generated by the permutations of the variables,

B) de Jonquières' automorphisms:

$$f(x_1, \dots, x_n) = (x_1, \dots, x_{n-1}, cx_n + P(x_1, \dots, x_{n-1})) \text{ with } c \neq 0.$$

It is known that all automorphisms of $k[2]$ are tame (see [Ju] and [Ku]). It is only a conjecture in more variables, see [BCW] and [N] for further details on the subject. We will see that we have a good bound on the degree of canonical bases for automorphisms of $k[2]$.

PROPOSITION 11. — *If f is an automorphism of $k[2]$, we can be in the two following situations:*

A) there exists some integer a such that $\mathrm{mdeg} f_1 = a \mathrm{mdeg} f_2$ *or* $\mathrm{mdeg} f_2 = a \mathrm{mdeg} f_1$,

B) $\{f_1, f_2\}$ is a canonical basis of $k[2]$.

PROOF. Using the fact that f is tame we have $f = g_h \circ \cdots \circ g_1$ where the g_i are elementary. It is then easy to prove the result by induction on h. ∎

COROLLARY 1. — *With the same notations, the canonical basis may be computed without considering any superposition of multidegree greater than* $\max(\mathrm{mdeg} f_1, \mathrm{mdeg} f_2)$.

PROOF. If we are in situation A), we can remark that the first superposition will be for example a reduction of $f_1 \xrightarrow{f_2} f_3$ of multidegree $\mathrm{mdeg} f_1$, so that we can delete f_1 and continue with f_2 and f_3. As the reduction corresponds to a de Jonquières' automorphism $k[f_1, f_2] = k[f_2, f_3]$ and we can iterate the argument until we are in case B). Then we have secured a canonical basis, and the bound holds for the multidegrees of $f_1, f_2, \dots$ are decreasing. ∎

Remark 2. — By the same proof, we see that the canonical basis algorithm will split f as a composition of elementary automorphisms.

It would be tempting to try to generalize prop 2. This can be done in the following way.

PROBLEM. *Let f be a tame automorphism of $k[n]$, does it exist $i \in [1, n]$ such that*

$$\mathrm{mdeg} f_i \in \mathrm{Mon} k[f_1, \dots, \widehat{f_i}, \dots, f_n]?$$

If we had a positive answer to that problem, we would be able to split f using canonical bases computations. But we would not have any more the bound of cor. 3, for we do not even know if the canonical basis of $k[f_1, \dots, \widehat{f_i}, \dots, f_n]$ is finite—as it is integrally closed, it would be a consequence of our conjecture p. 65.

The study of this problem has a special interest, for there is an automorphism of $k[x, y, z]$, given by NAGATA in [N], which does not match its conclusion, so that if the result holds anyway, the tame generators conjecture would be false in 3 variables.

Example 1. — (Nagata 1972) If we consider the automorphism

$$f : \begin{array}{lcc} x & \mapsto & x - 2y(y^2 + xz) - z(y^2 + xz)^2 \\ y & \mapsto & y + z(y^2 + xz) \\ z & \mapsto & z, \end{array}$$

we can see that for all orderings, we cannot have $\mathrm{mdeg} f_i \in \mathrm{Mon} k[f_j, f_k]$ with all different indices. The consideration of this example convinced NAGATA that the tame generators conjecture is false.

We will conclude by giving a class of tame automorphism, for which the answer to our problem is yes.

DEFINITION 17. — *We say that f is a generic tame automorphism of $k[n]$ if $f = g_h \circ \cdots \circ g_1$, where the g_i are elementary automorphisms such that:*

a) g_{2j+1} is de Jonquières and the polynomial P is dense dense and of degree at least 2,

b) all coefficients are algebraically independent on the ground field of k,

c) g_{2j} is a permutation which do not leave x_n invariant.

PROPOSITION 12. — *If f is a generic tame automorphism of $k[n]$, then the f_i form a canonical basis or there exist $i \in [1, n]$ such that* $\mathrm{mdeg} f_i \in \mathrm{Mon}\{\mathrm{mdeg} f_j | j \neq i\}$.

PROOF. If f is defined as in def. 16, this is easily proved by induction on h. ∎

COROLLARY 1. — *If f is a generic tame automorphism, then it can be split into a composition of elementary automorphism by a canonical basis algorithm where no superposition of multidegree greater than* $\max\{\mathrm{mdeg} f_i\}$ *needs to be considered.*

PROOF. The proposition implies that if the f_i do not form themselves a canonical basis, then the canonical basis may be computed by successive reductions. ∎

Of course, in practice we will consider automorphism defined by polynomials in $\mathbf{Q}[n]$. But it seems, by trying many examples, that the "average" complexity will be the same, the computational time being of the same order than the time needed to build f as a composition of elementary automorphisms.

Example 2. — Consider the set of polynomials $\{x, y + x^{10}, z + y^{10}, t + z^{10}\}$. It determines a tame automorphism of $k[x, y, z, t]$ and that can be tested in 1.1s using Scratchpad on a IBM 4381. The computation of the standard basis of Shannon and Sweedler's method takes 496.9 seconds using the pure lexicographical ordering.

Of course, in such an example where the inverse is of degree 1000, a method which determines it needs to get in some troubles. In cases where f and f^{-1} have the same degree, standard bases are more efficient in small examples, but canonical bases are better when the degree increases.

7. Relation avec le formalisme général

En ce qui concerne les bases canoniques, il suffit de prendre pour $\mathcal{B}'$ la structure de monoïde et pour $\mathcal{B}$ celle de k-algèbre. On n'a guère besoin d'une structure $\mathcal{A}'$, qu'on peut donc choisir vide, pour respecter les formes. On a cependant besoin d'une application f, qui à tout élément de l'algèbre associe 1, car $a^0 = 1$ est purement conventionnel. On pourrait être plus subtil, et prendre pour A l'ensemble des polynômes en une variable sur k, avec

$$\begin{array}{rccc} \diamond: & A \times B & \mapsto & B \\ & (P, Q) & \mapsto & P(Q). \end{array}$$

On n'a alors plus besoin de f. Les structure $\mathcal{A}$ et $\mathcal{A}'$ sont alors respectivement confondues avec $\mathcal{B}$ et $\mathcal{B}'$.

Pour la généralisation des bases standard, comme dans le cas habituel, il faut prendre pour $\mathcal{A}$ celle de k-algèbre, et pour $\mathcal{A}'$ celle de monoïde, pour $\mathcal{B}(A)$ la structure de A-module, pour $\mathcal{B}'(A')$ celle de “monomodule” sur A', c'est-à-dire d'ensemble avec une action du monoïde A'.

§ 4. EXEMPLES ET TEMPS D'ÉXÉCUTION

On va donner quelques exemples et des temps d'éxécution correspondant aux diverses méthodes décrites au cours de ce chapitre. Il ne s'agit que de quelques éléments partiels, mais qui permettent de préciser et de relativiser l'information fournie par les bornes théoriques. Généralement, les choses se passent mieux que ne le laisse craindre la borne de Gabber.

1. Un exemple d'application rationnelle inversible

Cet exemple n'a pas de rapport avec l'identifiabilité. Il provient d'un problème de physique qui, mal posé, se présente sous la forme suivante. On considère l'application rationnelle

$$\begin{array}{ccc} f: \quad \mathbf{C}^9 & \mapsto & \mathbf{C}^{12} \\ (x_{\ell,m}\ 1 \leq \ell, m \leq 3) & \mapsto & (S_{i,j,k}\ 1 \leq i,j,k \leq 3\ j,k \neq i), \end{array}$$

où

$$S_{i,j,k} = x_{j,k} + \frac{x_{j,i}x_{i,k}}{g_i - x_{i,i}},$$

les g_i étant des constantes supposées génériques. On veut déterminer si f possède un inverse rationnel et le déterminer.

On a d'abord utilisé la méthode de l'idéal Δ pour tester l'existence de l'inverse. On travaille dans le corps $\mathbf{Q}(g_1, \ldots, g_3)$, et l'on prend une variable u_i par numérateur, ayant remarqué qu'il n'y avait que 3 numérateurs distincts. On peut alors calculer la base standard de l'idéal $\mathcal{J}$ défini au th. 2.1.2 p. 50 en 43 sec. avec Scratchpad II.

Avec G. Moreno, on a simulé la méthode du graphe avec MACAULAY sur SPS7 Bull, pour obtenir l'expression de l'inverse. Mais le calcul a échoué après plusieurs jour de calcul, par saturation de la mémoire. En SCRATCHPAD II sur IBM 4381, la situation est encore plus deésespérée : on épuise l'espace disponible en 10 min. En fait un problème d'inversion de matrice est caché derrière ces fractions rationnelles. C'est pourquoi l'inverse est difficile a calculer de cette manière brutale.

En effet, on peut remarquer que l'application $M \mapsto M^{-1}$ pour une matrice carrée générique de taille n definit une application birationnelle involutive $f\colon \mathbf{A}^{n^2} \mapsto \mathbf{A}^{n^2}$, dont l'expression sous forme de fraction est de grande taille. La force brutale des méthodes automatiques ayant échoué, il a fallu revenir à l'origine du problème pour le résoudre et le comprendre, dans le cadre d'un travail commun avec M. Giusti.

Ceci montre bien en revanche la force de la méthode reposant sur le calcul d'une base standard de l'idéal Δ qui peut conclure ici en un temps modéré parce qu'elle évite absolument de calculer l'inverse. J'ai effectué quelques tentatives pour garder une trace des opérations effectuée sur le corps de base pendant le calcul de la base, qui aurait pu fournir, une fois simplifiée un "programme" de calcul de l'inverse. Mais la taille de cette trace s'est avérée, elle aussi, rédhibitoire.

Si l'on ne prend qu'une varibale u, avec le produit de dénominateurs, le temps de calcul augmente notablement, puisqu'il faut alors 247.62 sec. Ce résultat reste difficile à interprèter, mais se trouve confirmé par bien d'autres exemples.

2. Exemples d'applications polynomiales "apprivoisées"

À défaut de connaître des exemples sauvages, on va comparer les méthodes s'appliquant dans le cas polynomial sur deux classes remarquables d'automorphismes apprivoisés.

Exemples. — 1) Dans cet exemple, on considère la famille d'applications $f_i\colon \mathbf{A}^i \mapsto \mathbf{A}^i$ définies par

$$f_i(x_1, \ldots, x_i) = (x_1, x_2 + x_1^3, \ldots, x_i + x_{i-1}^3).$$

On l'a testée avec les trois méthodes suivantes :

(Γ) on utilise la méthode de l'idéal $(\Gamma) = (f_i(x) - y_i)$ (§ 2 n° 1) avec l'ordre lexicographique pur sur $x_1, \ldots, x_i, y_1, \ldots, y_i$, et le package de bases standard de Scratchpad II, implanté par Gebauer et Moeller,

(Σ) on utilise la méthode de l'idéal $\Sigma = (f_{i(x)-f_i(y)}$ (§ 2 n° 2) avec l'ordre degré puis lexicographique inverse sur $x_1, \ldots, x_i, y_1, \ldots, y_i$, et le même package de bases standard,

(C) on utilise cette fois le package de bases canoniques que j'ai implanté en Scratchpad II, avec l'ordre degré puis lexicographique inverse sur $x_1, \ldots, x_i$.

Le tableau suivant résume les résultat obtenus. Le signe †signifie que le calcul a été interrompu par saturation de la mémoire.

Temps d'exécution en secondes						
	f_2	f_3	f_4	f_5	f_6	f_7
(Γ)	0,1	0,5	1,0	38,7	†	†
(Σ)		0,5	0,55	0,65	0,8	1,0
(C)	1,0	1,1	1,3	1,9	2,5	5,9

Tableau 1.

On remarque que sur cette classe d'exemple, (Σ) est la meilleure méthode. Ceci se comprend assez bien, car l'algorithme de base standard tend dans ce cas à réduire continument la taille des polynômes présents. Les bases canoniques (C) donnent des temps eux aussi réduits. L'algorithme se résume dans ce cas à une suite de réductions. Expliquer pourquoi cette méthode est cependant moins bonne que (Σ) réclammerait des investigations plus profondes. En première analyse, on peut l'imputer au calcul de base standard nécessaire pour trouver les superpositions.

Il est logique que la méthode (Γ) sature assez vite la mémoire, car elle calcule explicitement f_i^{-1} qui est de degré 3^{i-1}.

2) La deuxième classe d'exemples est "orthogonale" à la première. En effet on considère l'application

$$\begin{array}{rccc} g\colon & \mathbf{A}^2 & \mapsto & \mathbf{A}^2 \\ & (x,y) & \mapsto & (y+x^3,y), \end{array}$$

dont l'inverse est aussi de degré 3. On a testé successivement l'inversibilité de g, g^2, etc. avec les mêmes méthodes que pour l'exemple précédent.

Temps d'exécution en secondes					
	g	g^2	g^3	g^4	g^5
(Γ)	0,32	0,36	0,9	23,6	1192,3
(Σ)	0,31	0,35	1,45	819,7	†
(C)	0,35	0,58	1,0	6,65	342,1

Tableau 2.

On remarque qu'ici ce sont les bases canoniques qui l'emportent. En un sens, le temps de calcul est optimal dans la mesure où il est très voisin du temps nécessaire pour calculer g^i. Ceci se comprend aisément, car une fois encore le calcul de base canonique se résume à une suite de réductions, consistant à "inverser" les évaluations correspondant au calcul de g^i. Le degré et la taille des résultats intermédiaires décroissent donc strictement au cours du calcul. Le temps supplémentaire nécessaire pour calculer les S-polynôme par un calcul de base standard est ici négligeable, car la croissance rapide de la taille des polynômes — g^i est de degré 3^i — rend le coût des évaluations prépondérant.

La méthode du graphe se comporte relativement bien, car la base standard qu'elle retourne a une taille strictement équivalente à celle des polynômes générateurs, 3^i, ce qui l'empêche d'exploser comme dans l'exemple précédent.

La plus mauvaise méthode est cette fois (Σ). Ce résultat était pour moi inattendu, et je n'ai pas d'explication précise. Le résultat final $\{x_i - y_i\}$ est de taille négligeable, et le degré ne dépasse pas celui des générateurs en cours de calcul. Un élément d'explication est peut-être que les générateurs sont de plus grande taille que pour Γ, ce qui alourdit le début du calcul.

Ces deux exemples d'aspect un peu paradoxal permettent d'encadrer l'ensemble des cas de figure. La méthode Σ semble préférable si l'inverse est de haut degré par rapport à l'application directe, auquel cas, la méthode Γ a toute chance d'échouer.

En revanche, lorsque les degré de f et f^{-1} coïncident, on peut utiliser Γ alors que Σ est notablement ralentie et plus gourmande en mémoire.

Les bases canoniques me semblent fournir la méthode qui se comporte généralement le mieux.

CHAPITRE IV

Bases standards. Ensembles caractéristiques

§ 1. BASES STANDARD D'IDÉAUX DIFFÉRENTIELS

1. Introduction

L'algorithme de calcul d'ensembles caractéristiques introduit par RITT utilise la noetherianité de l'ensemble des idéaux radiciels, mais il ne permet de tester l'appartenance d'un polynôme à un idéal que dans le cas où cet idéal est premier. D'autre part, il n'est que partiellement effectif, dans la mesure où il nécessite des factorisations. Un meilleur algorithme, n'utilisant que les opérations du corps de base, si celui-ci est de caractéristique 0, a été développé par SEIDENBERG (cf [Sei]) en 1956. Il a été récemment implantée par Sette DIOP (cf. [Di]) qui l'a appliqué à des problèmes d'automatique. Toutefois, cette approche résoud en fait un problème plus complexe, qui est de caractériser la projection ensembliste d'une variété algébrique différentielle affine, alors que dans de nombreux cas, la connaissance de son adhérence peut suffire. Comme on ne s'intéresse ici qu'à des idéaux premiers, on peut aussi se contenter des ensembles caractéristiques de Ritt dont un algorithme de calcul sera donné au § 2. Cette notion dérive des travaux de RIQUIER et JANET, ce dernier auteur n'étant jamais cité par Ritt !

On va introduire une notion de bases standard pour les idéaux différentiels, en utilisant le formalisme de III.1. Il n'est sans doute pas inutile de préciser qu'il ne s'agit pas d'une nouvelle mouture de la théorie des bases standard pour les $\mathcal{D}$-module, initiée par les travaux de BRIANÇON, CASTRO, GALLIGO, MAISONOBE (voir par exemple [Cas] ou [Gal]). On pourra cependant se convaincre que les bases standard de $\mathcal{D}$-modules entrent aussi dans notre formalisme. En revanche, la notion de base standard d'idéaux différentiels a déjà été introduite par Giuseppa CARRÁ FERRO (cf. [Car1]), et en dépit d'une présentation différente, il s'agit bien de celle qui va être exposée et que j'ai retrouvée indépendamment. Un des avantages de cette exposition est d'autoriser une classe d'ordres admissibles beaucoup plus large, et d'être plus directe dans la mesure où elle introduit d'emblée un ensemble de S-polynômes, provenant de syzygies différentielles, plutôt que de procéder par des calculs répétés de bases standard algébriques.

Comme on l'a dit au chapitre I p. 7, la différence essentielle est qu'on se place ici sur un anneau non-noetherien, mais commutatif. Ce dernier point simplifie les choses, mais la perte de la noetherianité pose des problèmes beaucoup plus graves. En effet, comme on doit semble-t-il s'y attendre dans une telle situation, les bases standard ne seront pas en général finies, mêmes pour des idéaux de type fini ; on a déjà rencontré ce type de difficultés avec les bases canoniques de sous-algèbre. Apparemment, les mauvais cas sont ici beaucoup plus fréquents, et sont peut-être la règle, car même un idéal engendré par un monôme sur une algèbre de polynômes différentiels en une seule variable peut avoir une base standard infinie ; c'est le cas pour l'idéal $[x^2]_{\mathcal{F}\{x\}}$ où $\mathcal{F}$ désigne un corps différentiel ordinaire. Cet exemple, qui est le plus simple qu'on puisse donner, est aussi dans l'article [Car1]. De plus, l'ensemble des syzygies à considérer peut être lui-même infini.

On peut dès lors douter de l'intérêt de ces bases standard. On peut avancer deux types de justifications. D'une part, si l'idéal est homogène pour le poids et si les dérivations sont triviales sur le corps, le calcul de la base standard jusqu'à un poids fixé permet de répondre au problème de l'appartenance pour tous les polynômes de poids inférieur, ce que les autres méthodes ne peuvent pas faire en général. D'autre part, l'existence éventuelle de bornes sur l'ordre de dérivation des générateurs pour exprimer un polynôme de l'idéal d'un poids donné permettrait de majorer l'ordre de complexité des calculs, tandis que la complexité des calculs d'ensembles caractéristiques est très difficile à évaluer, même dans le cas algébrique. On verra que l'analogue différentiel du théorème de Gabber, nous donnera une borne pour la détermination effective des automorphismes de $\mathcal{F}\langle n\rangle$ par un calcul de bases standard. Plus généralement, un nullstellensatz différentiel permettrait dans de nombreux cas de majorer la complexité des calculs. Enfin, il n'est sans doute pas inutile, pour mieux connaître les possibilités et les limites des techniques de réécriture en algèbre effective, d'évaluer les potentialités de cette généralisation, peut-être brutale.

Le formalisme de III.1 serait assez puissant pour définir des bases standard d'idéaux différentiels en caractéristique positive. Ce raffinement n'étant pas essentiel, surtout pour des applications à l'automatique, on peut, comme pour les bases canoniques, oublier l'élément $\top$ et les complications qu'il introduit. Les extensions possibles seront indiquées brièvement à la fin du paragraphe.

La suite de ce paragraphe reprend en partie le texte non traduit de l'article [O3], à l'exception de quelques résultats déjà introduits dans les chapitres I et II.

2. Standard bases

We will denote by $\mathcal{F}$ a differential field of characteristic 0.

2.1. Admissible orderings. Reduction

We need to define suitable orderings to allow reductions in $\mathcal{F}\{X\}$. This implies to strengthen the definitions valid in the pure algebraic case in order to take derivations into account.

DEFINITION 1. — *Let $<$ be a total ordering on the set $\mathcal{M}$ of monomials of $\mathcal{F}\{X\}$. We extend derivations to $\mathcal{M}$ by taking δM to be the maximal monomial involved in the polynomial δM. By convention, $\delta\, 1 = 1$. The order $<$ is said to be admissible if*

a) $M > 1$ $M \neq 1$,
b) $M > M'$ *implies* $M''M > M''M'$,
c) $\delta M > M$ $M \neq 1$,
d) $M > M'$ *implies* $\delta M > \delta M'$.

If $<$ is admissible, we denote by $\mathrm{m}P$ *the primitive leading monomial of P, by* $\mathrm{lc}P$ *its leading coefficient. We call reductum of P the polynomial* $P - \mathrm{lc}\,P\,\mathrm{m}\,P$.

So we define $\delta\, M$ in $\mathcal{M}$ to be $\mathrm{m}(\delta\, M)$. I think no misunderstanding can result of this abuse of notation, which allows to simplify formulas.

We now need to describe some admissible orderings. For this, we first define admissible orderings, i.e. rankings in the words of Ritt, on the set of derivatives $\Theta\, X$. They are orderings which satisfy c) and d) in the definition above. Considering elements of Θ as monomials, e.g. in $\mathbf{Q}[\Delta]$, we take an admissible ordering on Θ. We extend it to $\Theta\, X$ with the following definitions.

DEFINITION 2. — *The ordering on $\Theta\, X$ defined by $x_{i,(\theta)} < x_{i',(\theta')}$ if $i < i'$ or $i = i'$ and $\theta < \theta'$ is said to be the lexicographical ordering extending $<$.*
The ordering defined by $x_{i,(\theta)} < x_{i',(\theta')}$ if $\theta < \theta'$ or $\theta = \theta'$ and $i < i'$ is the derivation ordering extending $<$.

It is easily seen that those orderings are admissible (see [Ko chap. 0 §17 p. 50]).

Remark 1. — If $<$ on Θ respects the order, then the derivation ordering $<$ on $\Theta\, X$ respects the order too, it is said then to be *orderly*.

Let $<$ be an admissible ordering on derivatives, we can extend it to monomials of $\mathcal{F}\{X\}$ in the following way. Consider two monomials $M = \prod_{i=1}^{r} v_i^{\alpha_i}$ and $M' = \prod_{i=1}^{s} \nu_i^{\beta_i}$, where the v_i and ν_i appear in strictly decreasing order. We take $M < M'$ if there exist $j \leq r, s$ such that $v_i = \nu_i$ $i < j$, $\alpha_i = \beta_i$ $i < j$, $v_j < \nu_j$ or $v_j = \nu_j$ and $\alpha_j < \beta_j$. We will call this ordering the *pure lexicographical ordering* induced by the ordering $<$ on derivatives.

PROPOSITION 1. — *The ordering $<$ defined above is an admissible well ordering on monomials. If $<$ is orderly, its extension to monomials is also orderly, i.e.* $\mathrm{ord}\, P > \mathrm{ord}\, Q$ *implies* $P > Q$.

PROOF. It is immediate that a) and b) are satisfied. In order to prove c) and d), we only have to remark that $\delta\, m = \delta\, v_1\, v_1^{\alpha_1 - 1} \prod_{i=2}^{r} v_i^{\alpha_i}$. If $<$ is orderly on derivatives, then $\mathrm{ord}\, P < \mathrm{ord}\, Q$ implies that the leading derivative of P is smaller than that of Q, so that $P < Q$.

We now show that $<$ is a well ordering. It is known that all admissible orderings on variables are well orderings (see [Ko]). Consider now an infinite sequence $M_0 > M_1 > \cdots$ of monomials. The leading derivatives of these monomials appear in decreasing order, so that for some integer r the chain they form will become stationary. Let v be the leading derivative of M_i for $i > r$. The degree in v of M_i $i > r$ will be decreasing too, so that for $i \geq s \geq r$ this degree becomes a constant integer d. Dividing M_i by v^d, for $i \geq s$, we secure a new strictly decreasing sequence of monomials, whose leading derivatives are smaller than v. Repeating the argument, we build an infinite strictly decreasing sequence of derivatives: a contradiction. ∎

So admissible orderings on monomials actually exist. It will be useful to consider other orderings than those coming from the previous propositions. We may first remark that if P is a differential polynomial of degree d, then θP is also of degree d, moreover if P is homogeneous, θP is homogeneous too. We shall need some more convenient gradings on $\mathcal{F}\{X\}$, for example the weight (see déf. I.2.2.3 p. 7).

Lemma 1. — *If $<$ is an admissible ordering on monomials, we get a new admissible ordering $\prec$ by taking $M \prec M'$ if $\deg M < \deg M'$ or if $\deg M = \deg M'$ and $M < M'$. The same applies when considering the weight, or the partial degree according to some subset of X.*

If $<$ is a well ordering, then $\prec$ is also a well ordering ■

Remark 2. — More generally, we can use all the admissible gradings defined in [Ko chap I §7 p. 72] (see I.2.2), and then refine them by using the pure lexicographical ordering induced by an ordering $<$ on derivatives, or the inverse ordering.

Recursive use of this lemma allows to build a wide class of orderings, for example elimination orderings. In the following, we will suppose that such an ordering $<$ has been chosen once and for all.

We know that admissible orderings for algebraic standard bases have been classified by ROBBIANO. Recently, G. CARRA'FERRO has announced she managed to classify admissible orderings on derivatives ([Car3]). It would be very interesting to try to extend those works to admissible orderings on differential monomials.

We now come to reduction.

DEFINITION 3. — *We say that a polynomial P is elementarily reduced by Q to R if there exist a monomial M and a derivation operator θ such that $\mathrm{m}\, P = M\, \mathrm{m}\, \theta\, Q$ and $R = P - (\mathrm{lc}\, P/\mathrm{lc}\, Q)\, M\, \theta\, Q$. We write it $P \xrightarrow{Q} R$. We say that P is elementarily reduced to R by a set of polynomials Σ if there exist $Q \in \Sigma$ such that $P \xrightarrow{Q} R$. P will be said to be reduced to R by Σ if there exist a chain of elementary reductions*

$$P = P_0 \xrightarrow{\Sigma} P_1 \xrightarrow{\Sigma} \cdots \xrightarrow{\Sigma} P_r = R.$$

We denote it by $P \xrightarrow{\Sigma^\star} R$.

We say that P is totally reduced to R by Σ if P is reduced to R by Σ or if the reductum of P is totally reduced to R' by Σ and $R' = lc\, P\, \mathrm{m}\, P + R'$. P is irreducible by Σ if there is no Q such that $P \xrightarrow{\Sigma} Q$.

Remark 3. — If we use the fact that $\theta\, \mathrm{m}\, P = \mathrm{m}(\theta\, P)$, for $P \notin \mathcal{F}$, with the extension of derivations to monomials made above, it becomes obvious that the reducibility of P by Q only depends of the leading monomials of P and Q. It is easily seen then that, if P is reducible by Q, the weight (or degree) of the leading monomial of P is not less than that of Q. It is also obvious that $P \xrightarrow{Q} R$ implies $\mathrm{m}\, R < \mathrm{m}\, P$.

Lemma 2. — *$P \xrightarrow{\Sigma^\star} 0$, iff $P = \sum_{i=1}^{r} M_i\, \theta_i\, P_i$, where the M_i are terms, and the P_i polynomials in Σ, with $\mathrm{m}(M_i\, \theta_i\, P_i) > \mathrm{m}(M_j\, \theta_j\, P_j)$ $i < j$.* ■

We can build an effective reduction process which takes a polynomial P and a finite list of polynomials Σ and returns a polynomial R such that $P \xrightarrow{\Sigma^*} R$ and R is irreducible by Σ. We begin by reduction with respect to a single polynomial. We use the syntax of the IBM computer algebra system Scratchpad II for the algorithms.

REDUCTION ALGORITHM

```
reduction(P, Q) == reduction(P, Q, 1)
reduction(P, Q, r) ==
  deg m P > deg m Q or wt m P > wt m Q => return P
  m Q\m P => return reduction(P − (lc P/lc Q) (m P/m Q) Q, Q)
  for i ∈ [r, ..., m] repeat
    if (P2 := reduction(P, δi Q, i)) ≠ P then return reduction(P2, Q)
  P
```

PROOF. We first prove that the process stops and return P if it is irreducible by Q. If we can apply the remark above, it stops on the first line. If not, the process is recursively repeated with derivatives of P. As their weight increases by 1 at each new step, the remark will necessarily apply after a finite number of steps. Now, if P is reducible, its leading monomial needs to be a multiple of the leading monomials of some $\theta\, Q$. A solution will to be found by trying all successive derivatives of Q, whose leading monomials have weight less or equal to the weight of P, which is done. We perform then an elementary reduction, and repeat the process. It needs to stop, for $<$ is a well ordering, and so there is no infinite sequence of elementary reductions. ∎

It is now simple to get a reduction algorithm for a list of polynomials, or for total reduction.

2.2. Definitions

DEFINITION 4. — *Considering the multiplicative monoïd $\mathcal{M}$ of monomials in $\mathcal{F}\{X\}$, with the derivations acting on it as in def. 2.1.1 p. 77, we call a subset E a differential monoïdeal if it is a monoïdeal—i.e. if $\mathcal{M}E \subset E$—, and if $\Delta\, E \subset E$.*

Remark 4. — Obviously, the set of leading monomials of a differential ideal is a differential monoïdeal—because we are in characteristic zero. Of course the "derivations" defined on $\mathcal{M}$ are not real ones, but the mere reflect of derivations acting on polynomials. Indeed, the mapping δ_i themselves do not need to be derivations. We only need that $\mathrm{m}\delta\, P = \mathrm{m}\delta(\mathrm{m}\, P)$ and that $\delta(P+Q) = \delta\, P + \delta\, Q$, so that we could use more general differential operators, say $d = \delta_1^2 - \delta_2^3$ and define standard bases for d-ideals, i.e. ideals $\mathcal{I}$ such that $d\mathcal{I} \subset \mathcal{I}$, but for this we would need a more complicated definition of reduction, and a wider class of syzygies (see n° 4 bellow).

Using derivations, we are indeed able to restrict the set of syzygies to consider, for given a product of monomials $M\, M'$, $\delta(M\, M')$ equals $\delta\, M\, M'$ or $M\,\delta\, M'$, so that the differential monoïdeal generated by a subset E of $\mathcal{M}$ is equal to $\mathcal{M}\,\Theta\, E$ (see n° 2.4 bellow).

DEFINITION 5. — *A subset G of a differential ideal $\mathcal{I}$ is said to be a standard basis if $\mathrm{m}\, G$ generates $\mathrm{m}\,\mathcal{I}$ as a differential monoïdeal.*

THEOREM 1. — *Let G be a set of polynomials, $\mathcal{I}$ a differential ideal. Then the following propositions are equivalent:*

i) G is a standard basis of $\mathcal{I}$,

ii) $G \subset \mathcal{I}$ and there is no non-zero element of $\mathcal{I}$ reduced with respect to G,

iii) $G \subset \mathcal{I}$ and all the elements of $\mathcal{I}$ are reduced to 0 by G,

iv) a differential polynomial is in $\mathcal{I}$ iff it is reduced to 0 by G.

PROOF. *i)* $\Longrightarrow$ *ii)*. If G is a standard basis of $\mathcal{I}$ it is a subset of $\mathcal{I}$. Now, the leading monomial of any non-zero polynomial in $\mathcal{I}$ is in $\mathcal{M}\,\Theta\,\mathrm{m}\,G$ using the remark above, so that it is reducible by G.

ii) $\Longrightarrow$ *iii)*. As $G \subset \mathcal{I}$, if $P \xrightarrow{G} Q$ with $P \in \mathcal{I}$, then $Q \in \mathcal{I}$, so that we can perform repeated reductions using ii). As chains of reductions are finite, *the result of any reduction process* is 0, which is more than iii).

iii) $\Longrightarrow$ *iv)*. $\Rightarrow$ is immediate from iii). $\Leftarrow$ Again, as $G \subset \mathcal{I}$, if $P \xrightarrow{G^*} 0$, P needs to be in $\mathcal{I}$.

iv) $\Longrightarrow$ *i)*. All polynomials in G are reduced to 0 by G, so that $G \subset \mathcal{I}$. As all polynomials in $\mathcal{I}$ are reduced to 0 by G, they are reducible, so that $\mathrm{m}\,\mathcal{I} \subset \mathcal{M}\,\Theta\,\mathrm{m}\,G$. Using the first part of the proof, we have indeed equality. ∎

DEFINITION 6. — *A standard basis G of $\mathcal{I}$ is said to be minimal if $\mathrm{m}\,G$ is a minimal set of generators of $\mathrm{m}\,\mathcal{I}$. A minimal standard basis G is called reduced if all polynomials $P \in G$ are totally reduced by $G \setminus \{P\}$.*

PROPOSITION 2. — *Any ideal admits minimal standard bases and a unique reduced standard basis. An ideal admits a finite standard basis iff it admits a finite minimal standard basis. In this case, all the minimal standard bases are finite.* ∎

2.3. Characterization

We have completed the easiest part with definitions. The completion process will rely on more tedious results.

DEFINITION 7. — *Let P and Q be two differential polynomials, we call a syzygy between P and Q a 2-uple $(M\,\theta\,P, M'\,\theta'\,Q)$, where $M, M' \in \mathcal{M}$, $\theta, \theta' \in \Theta$, of polynomials with the same leading monomials. An essential syzygy is a syzygy with M and M' minimal and such that there is no other syzygy $(N\,\tau\,P, N'\,\tau'\,Q)$ satisfying $\vartheta(N\,\tau\,\mathrm{m}\,P) = M\,\theta\,\mathrm{m}\,P$ and $\vartheta(N'\,\tau'\,\mathrm{m}\,Q) = M'\,\theta'\,\mathrm{m}\,Q$ for some ϑ, the derivations being taken in $\mathcal{M}$.*

We call S-polynomial associated to the syzygy (U, V), the polynomial $\mathrm{lc}\,V\,U - \mathrm{lc}\,U\,V$. The rank of the syzygy will be the common leading monomial of U and V.

Example 1. — Consider ordinary differential polynomials in $\mathcal{F}\{x\}$. There is only one admissible ordering on Θ and $\Theta\,x$. We choose then the pure lexicographical ordering on monomials it induces (see prop. 2.1.1 p. 77). Take $\mathcal{I} = \{x^2\}$. There is an essential syzygy $(\delta x\,x^2, x\,\delta(x^2))$. The syzygy $(\delta^2 x\,x^2, x\,\delta(x^2))$ is not essential. The only essential syzygies different from that already given are of the form $(\delta n + 1 x\,\delta^n(x^2), \delta^n x\,\delta^{n+1}(x^2))$ $n \geq 1$. This shows that syzygies may involve twice the same polynomial, and that there is in general an infinite number of essential syzygies.

DEFINITION 8. — *Let Σ be a set of polynomials, P a polynomial in $[\Sigma]$. We call rank of P with respect to Σ the smallest monomial M such that*

$$P = \sum_{i=1}^{r} Q_i\, \theta_i\, P_i, \tag{1}$$

where the P_i belong to Σ, the Q_i are terms and $\mathrm{m}\, Q_i\, \theta_i\, P_i \leq M$.

Remark 5. — The rank of P is greater than or equal to the leading monomial of P. If P is reduced to 0 by Σ, it is equal to $\mathrm{m}\, P$. We may consider, e.g. $\Sigma = \{\delta_1 x + \delta_3 x, \delta_2 x + \delta_3 x\}$ and $P = \delta_1\delta_3 x - \delta_2\delta_3 x$, assuming pure lexicographical ordering on Θ with $\delta_1 > \delta_2 > \delta_3$. Then, P is of rank $\delta_1\delta_2 x > \mathrm{m}\, P$ with respect to Σ. If P is the S-polynomial associated to a syzygy between elements of Σ, then the rank of P is less than or equal to the rank of the syzygy. We can further notice that if P is of rank M, Q of rank N, then $Q\, P$ is of rank at most $N\, M$, and that $\theta\, P$ is of rank at most $\theta\, M$.

THEOREM 2. — *G is a standard basis of the differential ideal $\mathcal{I}$ iff G generates $\mathcal{I}$ and all the S-polynomials associated to the set of essential syzygies between elements of G are reduced to 0 by G.*

PROOF. $\Longrightarrow$ is obvious since S-polynomials are in $\mathcal{I}$.

The reciprocal is the consequence of the following more precise theorem. ∎

THEOREM 3. — *Let M be a monomial, Σ be set of polynomials, such that all S-polynomials associated to the set of essential syzygies between elements of Σ of rank less than or equal to M are reduced to 0 by Σ. Then, if P is of rank less than of equal to M with respect to Σ, P is reduced to 0 by Σ.*

PROOF. Suppose it is not so. Among the P of minimal rank N which do not satisfy the conclusion, we choose one with smallest r in formula (1) of def. 8. The integer r is greater than 1. If not, P would be reduced to 0 by P_1. Now, we may decompose the sum (1) in two parts, e.g. $P = R_1 + R_2$ with $R_1 = Q_1\, \theta_1\, P_1$ and $R_2 = \sum_{i=2}^{r} Q_i\, \theta_i\, P_i$. Obviously, R_1 and R_2 need to be reducible, for they admit a decomposition (1) with a sum of at most $r-1$ polynomials with leading monomials at most N. This implies that R_1 and R_2 has the same leading monomial and opposite leading coefficient, if not P would be reducible.

We first prove that r is greater than 2. If $r = 2$, the polynomial $P = Q_1\, \theta_1\, P_1 + Q_2\, \theta_2\, P_2$ is the product of a S-polynomial, by a non zero element of $\mathcal{F}$. Without loss of generality we may suppose it is a S-polynomial. If this syzygy is essential, P is reducible: a contradiction. If not, suppose Q_1 and Q_2 are not minimal. They admit a proper common factor L, and P/L is of rank smaller than N, so that it is reducible and so is P: another contradiction.

The last case is when there exists a syzygy (U, V) between P_1 and S_1 such that $N = \mathrm{m}\, \vartheta\, U = \mathrm{m}\, \vartheta\, V$ for $\vartheta \neq 1$. The rank of (U, V) is less than N, so that the S-polynomial S associated to (U, V) is reduced to 0. This implies that the rank of ϑS is $\vartheta \mathrm{m} S$, strictly less than N. Now, we may develop:

$$\vartheta\, S = a\, P + \text{a sum (1) of rank less than } N,$$

where $a \in \mathcal{F}$ $a \neq 0$. Hence P is of rank less than N: a final contradiction to $r = 2$.

Using lemma 2.1.2 p. 79, we may now decompose R_2 as a sum (1) $\sum_{i=1}^{s} Q'_i\,\theta'_i\,P'_i$, with $\mathrm{m}(Q'_i\,\theta'_i\,P'_i) > \mathrm{m}(Q'_j\,\theta'_j\,P'_j)$ $i < j$.

Let $T = Q_1\,\theta_1\,P_1 + Q'_1\,\theta'_1\,P'_1$, R_1 and R_2 having opposite leading terms $\mathrm{m}T < N$. Furthermore $r > 2$ implies that T is reducible, so that T is of rank less than N. If we write P as $T + \sum_{i=2}^{s} Q'_i\,\theta'_i\,P'_i$, we conclude that P is of rank less than $N = \operatorname{rank} P$. ∎

The main idea is very general and follows a scheme for the proof of analogous theorems in other generalizations of standard bases (see chap. III § 1, where the proof of prop. 2.3.3 p. 48 is very similar).

2.4. Completion process

We now have enough material for investigating a completion process. The first step is to build, or rather to enumerate a set of essential syzygies. Differential syzygies between elements of Σ are algebraic syzygies between elements of $\Theta\,\Sigma$. So we can use the criteria detecting useless syzygies valid in the algebraic case. We will mostly use two of them, as an illustration.

Criterion 1. — If $(M\,\theta\,P, N\,\tau\,Q)$ is an essential syzygy such that $M = \mathrm{m}\,\tau\,Q$, then the associated S-polynomial is reduced to 0 by the set $\{P, Q\}$. ∎

Corollary 1. — *If P and Q are polynomials whose leading monomials are linear, i.e. are mere derivatives $\theta\,x_i$ and $\tau\,x_j$, then if $x_i \neq x_j$ all syzygies between P and Q are reduced to 0 by $\{P, Q\}$. If $x_i = x_j$, then we only have to consider the syzygy $(\tau'\,P, \theta'\,Q)$, where τ' and θ' are such that $\tau'\,\theta = \theta'\,\tau = \gcd(\theta, \tau)$.* ∎

Criterion 2. — If $P, Q, R \in \Sigma$, $S = (U, V)$ is an algebraic syzygy between $\theta\,P$ and $\tau\,Q$, $\mathrm{m}\,\vartheta R$ divides the rank of S and the algebraic syzygies between $\theta\,P$ and ϑR, $\tau\,Q$ and ϑR are both reduced to 0 by Σ, then S is reduced to 0 by Σ. ∎

Criterion 3. — If some derivative $\theta\,P$ is reduced to 0 by Σ, no syzygy involving a derivative $\tau\,\theta\,P$ needs to be considered. ∎

This simply rephrases well known results for algebraic standard bases (see [Bu1]). We will give more details on the differential situation in n° 4.

In the following completion process, G is the list which tends to a standard basis as the process goes. It will be indeed a standard basis if it stops. L_1 is the list of polynomials or derivatives of polynomials already considered, and L_2 is the list of newly appeared polynomials or derivatives, which should be used to try new syzygies. L_3 is the list of polynomials coming from the reduction of S-polynomials.

We suppose that *buildSyz*(L_1, L_2) is a procedure which returns all algebraic syzygies between two of derivatives in the list L_2, or a derivative in L_1 and one in L_2; it uses criteria 1 and 2 to discard useless syzygies, when possible. The procedure *isRed(S)* returns P if the syzygy corresponds to the algebraic reduction of the derivative P and 0 otherwise.

We can also use crit. 1 cor. 1 to test if there is no more syzygies to consider. Except if the ideal is [1], this is the only way I know to reduce to a finite set of syzygies—we may imagine cases where the basis is finite and there is still an infinite number of syzygies to consider. Indeed the main example of ideals with finite standard bases are linear ones (see [Car1 cor. 5 p. 138]).

The procedure *linTestY*(L_1, L_2) returns *true* if the two following conditions are satisfied:

a) there is no more syzygies between elements of L_2 to consider, using cor. 1,

b) the leading derivatives of polynomials in L_2 are all strictly greater than the derivatives appearing in the leading monomials of polynomials in L_1.

Of course, we are sometimes lucky enough to build a finite standard basis *and* finish the completion process even in non-linear cases (see bellow ex. 5.3 p. 85).

COMPLETION PROCESS

```
completionProcess(Σ) ==
  -- First suppress 0 and remove duplicate polynomials
  Σ := removeDuplicates delete(0, Σ)
  -- If there is a constant polynomial it is finished
  for P ∈ Σ repeat if P ∈ ℱ then return [1]
  G := Σ; L1 := Σ; L2 := Σ; L3 := []
  while L2 ≠ [] repeat
  -- We use cor. 1 to test if all remaining syzygies may be discarded
    if linTest(L1, L2) then return G
    -- We construct new syzygies between "old" polynomials in L1 and "new" ones in L2,
       or two new polynomials in L2
    lSyz := buildSyz(L1, L2)
    for S ∈ lSyz repeat
      -- If the syzygy is the algebraic reduction of a derivative, all syzygies involving this derivative
         may be removed
      P := isRed(S); delete(P, G); delete(P, L1); delete(P, L2)
      if (R := reduction (sPol(S), L)) ≠ 0 then
        -- If non-zero, the reduction of the S-polynomial is kept in L3
        L3 := cons(R, L3)
        -- If R ∈ ℱ it is finished
        if R ∈ ℱ then return [1]
    G := append(G, L3)
    -- Derivatives already considered are appended to L1
    L1 := removeDuplicates append(L1, L2)
    -- New polynomials coming from the reduction of S-polynomials
       and new derivatives are collected in L2
    L2 := append(L3, [δ P|(δ, P) ∈ Δ × L2])
    L3 := []; output(G)
  G
```

THEOREM 4. — *If the process stops it returns a minimal standard basis G of $[\Sigma]$. Otherwise, let G_i denote the set of polynomials, which is returned by the process at the end of the i^{th} loop, then:*

a) $G = \bigcup_{i=1}^{\infty} G_j$ is a minimal standard basis of Σ,

b) $G' = \bigcap_{i=1}^{\infty} \bigcup_{j=i}^{\infty} G_j$ is a minimal standard basis.

PROOF. At the beginning, $G = \Sigma$, so G generates $[\Sigma]$. During the process, if a polynomial is removed from G, then its reduction is added to G. So G still generates $[\Sigma]$. In both cases, all the S-polynomials coming from syzygies between elements of G, which are not thrown away using the criteria are reduced to 0 by G, so that is is a standard basis using th. 2.3.2 p. 81.

For the same reason, $G_i \bigcup_{j=i}^{\infty} G_j$ is a standard basis for all i, so that $\mathrm{m}\, G_i$ generates $\mathrm{m}\,[\Sigma]$. So G' is also a standard basis. As a polynomial $P \in G'$ is irreducible by $G' \setminus \{P\}$, G' is minimal. ∎

Remark 6. — If we use an orderly ordering, or a ordering which respects the weight, we can modify this process to make it stop if there is no more syzygies to compute, with order or weight less than or equal to a given integer.

If think a few words are necessary to stress on the differences between the completion process given here, and the approach in [Car1]. G. Carrá-Ferro proceeds by repeated computations of algebraic standard bases, so that the same work may be done many times. We only have here one process based on reduction of differential syzygies, which do not appear in her paper.

This allows sometimes to prove we have secured a finite basis, simply because the process stops (ex. 5.3 p. 85 bellow), as she needs in all cases to rely on some a priori mathematical knowledge. Of course, those improvements are far to solve everything.

2.5. Examples

Before considering examples, a few remarks are necessary.

Remarks. — 7) The completion process only uses the operations of the ground field, so that the polynomials in the standard basis have coefficients in the subfield generated by the coefficients of the input polynomials.

8) If $\mathcal{I} = [P_1, \ldots, P_r]$, where the P_i are homogeneous, the standard basis, which is the limit of our construction process will be homogeneous, as well as the reduced standard basis of $\mathcal{I}$. The same apply with isobaric polynomials, if all their coefficients are constants. In such cases, the weight, or degree of the polynomials in any basis cannot be less than the minimal weight or degree of the generators. So, considering a finite set Σ of isobaric polynomials with constant coefficients, we only have to run the completion process up to $\mathrm{wt}\, P$ in order to test if P belongs to $[\Sigma]$.

9) Suppose we are given an ordinary differential ideal generated by a system of so-called pseudo-state equations, i.e. equations of the form :

$$\begin{aligned} x_{1,(r_1)} &= P_1(x_{1,(r_1-1)}, \ldots, x_1, \ldots, x_{n,(r_n-1)}, \ldots, x_n) \\ &\vdots \\ x_{n,(r_n)} &= P_1(x_{1,(r_1-1)}, \ldots, x_1, \ldots, x_{n,(r_n-1)}, \ldots, x_n). \end{aligned}$$

For any orderly ordering $\{x_{i,(r_i)} - P_i\}$ is already the reduced standard basis of the generated ideal, and the procedure given above will stop. It it also a characteristic set.

Example 2. — We consider the ideal $\mathcal{I} = [x^2]$ already given in [Car1], using the same ordering as in example 3.1 p. 80. Ritt has shown that $(u')^{2\,p-1}$ belongs to $[u^p]$, so that for all r, $x_{(r)}^q \in \mathcal{I}$ for some integer q, which is greater than 1, using remark 8 above. Furthermore, $x_{(r)}^q$ can only be reduced by a polynomial in the basis with leading monomial $x_{(r)}^s$ $s \le q$. As $x_{(r)}^s$ is the smallest monomial of weight $r\,s$, it is in the reduced basis. So $[x^2]$ has no finite standard basis.

This shows that standard bases may be actually infinite, and even worse that it may be indeed the general case, for this example is very simple.

Example 3. — We now consider $\mathcal{I} = [P]$, where $P = x^2 + x + 1$. The first syzygy which appears is $(x'\, P, x\, P')$. The associated S-polynomial is $x\, x' + 2\, x'$ which is reduced to $3/2\, x'$, using P'. We add x' to the basis. P' is reduced to 0 by x'. Using crit. 3, all syzygies involving $P^{(s)}$ $s \leq 1$ may be discarded. P and x' are mutually totally irreducible, and using crit. 4.1 p. 82, there is no syzygy involving only x'. Hence, the reduced standard basis of $\mathcal{I}$ is finite and equal to $\{x^2 + x + 1, x'\}$. In our process, P' is deleted from L_2. The only polynomial left in L_2 is x', and $L_1 = \{P\}$. So the process stops using *linTest*.

As shown by this example there also exist non-trivial ideals with a finite standard basis, *which may be found in a finite number of steps by our completion process.*

Standard bases are often used to perform elimination of a set of variables. If we are lucky enough to secure a finite standard basis for a suitable ordering, this also works in the differential case.

PROPOSITION 3. — *Let $\mathcal{I}$ be a differential ideal of $\mathcal{F}\{X\}$, Y a subset of X. Using lemma 1.1, we take any ordering $<$ on monomials and build a new ordering $\prec$ by considering first the degree of polynomials in the variables Y. If G is a standard basis of $\mathcal{I}$ for $\prec$, then the subset $G' = \{P \in G | \mathrm{m}\, P \in \mathcal{F}\{X \setminus Y\}\}$ is a standard basis of $\mathcal{I} \cap \mathcal{F}\{X \setminus Y\}$.*

PROOF. Due to the properties of $\prec$, all polynomials in G' are in $\mathcal{F}\{X \setminus Y\}$, and polynomials in this subring cannot be reduced by the elements of $G \setminus G'$. So a polynomial in $\mathcal{F}\{X \setminus Y\}$ is in $\mathcal{I}$ iff it is reduced to 0 by G'. We conclude using th. 4.5. ∎

3. Applications birationnelles

On considère une application rationnelle différentielle $f\colon \mathbf{A}^n_{\mathcal{F}} \mapsto \mathbf{A}^m_{\mathcal{F}}$, où $f_i = P_i/Q_i$. On va montrer qu'il est possible de tester algorithmiquement que f admet un inverse d'un ordre fixé et de le determiner effectivement.

Lemme 1. — *Soit $\Sigma = \{A_i(x)D_i(y) - B_i(x)C_i(y)\ i \in [1, \ell]\}$ des polynômes de $\mathcal{F}\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$, et $R/S \in \mathcal{F}\langle \ell \rangle$ une fraction dont le numérateur et le dénominateur sont d'ordre r, au plus, et telle que $S(A_i/B_i) \neq 0$ et $S(C_i/D_i) \neq 0$. Alors, il existe $E(x)H(y) - F(x)G(y) \in (\Theta_r \Sigma)$, tel que E/F représente la fraction $R(A/B)/S(A/B)$ et G/H représente $R(C/D)/S(C/D)$.*

PREUVE. Pour les besoins de la demonstration, on dira que $E(x)H(y) - F(x)G(y)$ *représente* R/S. Il suffit de prouver que si R/S et R'/S' admettent des représentant $E(x)H(y) - F(x)G(y)$ et $E'(x)H'(y) - F'(x)G'(y)$ dans $(\Theta_{\mathrm{ord}\, R/S}\, \Sigma)$, alors cR/S $c \in \mathcal{F}$, RR'/SS' et $R/S + R'/S'$ en admettent dans le même idéal, et que $\delta(R/S)$ $\delta \in \Delta$ en admet un dans $(\Theta_{\mathrm{ord}(R/S)+1}\, \Sigma)$. Ceci résulte de calculs aisés. Par exemple,

$$(E(x)F'(x) + E'(x)F(x))H(y)H'(y) - (G(y)H'(y) + G'(y)H(y))F(x)F'(x) \in (\Theta_{\mathrm{ord}(R/S)}\, \Sigma)$$

représente $(R/S) + (R'/S')$. De même,

$$\begin{aligned}&(\delta\, E(x)\, F(x) - \delta\, F(x)\, E(x))H(y)^2 - (\delta\, G(y)\, H(y) - \delta\, H(y)\, G(y))F(x)^2\\ &\quad \delta\,(E(x)H(y) - G(y)F(x)) + (H'(y)F(x) - H(y)F'(x))(E(x)H(y) - G(y)F(x)) \in (\Theta_{\mathrm{ord}(R/S)+1}\, \Sigma)\end{aligned}$$

représente $\delta(R, S)$. Les derniers calculs, immédiats, sont laissés au lecteur. ∎

THÉORÈME 1. — *Soit Σ l'ensemble de polynômes différentiels*

$$\{P_i(x) - Q_i(x)y_i \ i \in [1,n]\},$$

alors f admet un inverse d'ordre r ssi la base standard réduite de l'idéal algébrique

$$\mathcal{I}_r = \left(\Theta_r\Sigma\,;\left(\prod_{i=1}^{m} Q_i(x)\right)\ u-1\right)_{\mathcal{F}[\Theta_{r+\mathrm{ord}\, f}\, x, \Theta_{\mathrm{ord}\, f}\, y, u]},$$

pour un ordre qui élimine u puis élimine fortement les dérivées des x, contient pour tout $1 \leq i \leq n$ un polynôme de la forme $S_i(y)x_i - R_i(y)$.

Dans ce cas, les fractions R_i/S_i déterminent l'inverse.

PREUVE. $\Longrightarrow$ Le lemme 1 implique que si f admet un inverse d'ordre r, défini par des fractions R_i/S_i alors pour tout $1 \leq i \leq n$ le polynôme $S_i(y)V(x) - R_i(y)W(x)$ appartient à $\mathcal{I}_r$, avec $V(x)/W(x) = x_i$.

Maintenant, une nouvelle utilisation du lemme montre que $\mathcal{I}_r \cap \mathcal{F}\{x, y\}$ est le graphe de l'application rationnelle

$$g\colon (\Theta_{r+\mathrm{ord}\, f}\, x) \mapsto (\Theta_r\, f(x)),$$

et donc que $\mathcal{I}_r$ est premier et ne contient pas de polynôme non nul $P(x)$. Ceci implique que $S_i(y)x_i - R_i(y) \in \mathcal{I}_r$. Enfin R/S définissant l'inverse de f, $S_i(y) \notin \mathcal{I}_r$, et l'on peut supposer S_i et R_i irréductibles en les remplaçant éventuellement par leur réduction relativement à la base standard. Alors, $S_i(y)x_i - R_i(y)$ ne peut être réduit que par un polynôme de la base standard réduite ayant la même forme, car l'ordre élimine fortement les dérivées des x.

$\Longleftarrow$ Si de tels polynômes appartiennent à l'idéal, il suffit de montrer que $S_i(y) \notin \Gamma(f)$ pour conclure, en utilisant la prop. II.4.1.1 cor. 3 p. 34. Si $S_i(y) \in \Gamma(f)$, alors $S_i(f) = 0$. Utilisant le lemme 1 ci-dessus, ceci implique que $S_i(y)V(x) \in \mathcal{I}_r$, où V est un produit de puissances des Q_i, et donc que $S_i(y) \in \mathcal{I}_r$, ce qui est exclu par hypothèse.

En outre, par construction, S_i et R_i sont d'ordre r, au plus. ∎

Ce théorème donne un moyen effectif de vérifier l'existence d'un inverse d'ordre r. Un cas interressant est celui des applications $f\colon \mathbf{A}^n \mapsto \mathbf{A}^n$, pour lequel on peut utiliser l'analogue différentiel du théorème prouvé par Gabber.

COROLLAIRE 1. — *Une application rationnelle différentielle $f\colon \mathbf{A}^n \mapsto \mathbf{A}^n$ est birationnelle ssi la base standard algébrique de l'idéal $\mathcal{I}_{n\mathrm{ord}\, f}$ contient pour tout $1 \leq i \leq n$ un polynôme de la forme $S_i(y)x_i - R_i(y)$.*

PREUVE. Ceci résulte du théorème précédent et de la borne sur l'ordre de l'inverse th. II.3.3.5 p. 30. ∎

Remarque 1. — On a donné une méthode reposant sur le calcul d'une base standard algébrique. Toutefois, on se convaincra aisément que ces polynômes doivent apparaître au cours du calcul d'une base standard de l'idéal différentiel engendré par Σ et $(\prod_{i=1}^{m} Q_i)\, u - 1$, où l'on néglige les syzygies d'ordre supérieur à $r + \mathrm{ord}\, f$.

2) On peut aussi éviter de calculer une base standard réduite, et vérifier l'apparition de polynômes, dont les monômes dominants sont de la forme $m_i(y)x_i$, dans une base standard minimale.

Si le théorème précédent permet de déterminer algorithmiquement l'existence d'un inverse d'ordre r, on ne dispose pas d'une borne de complexité pour ce calcul. On va donner une méthode différente, utilisant l'idéal $\Delta(f)$, qui ne permet pas d'exprimer l'inverse mais pour laquelle on peut prouver une borne de complexité.

THÉORÈME 2. — *Soit $f\colon \mathbf{A}^n \mapsto \mathbf{A}^m$ une application rationnelle différentielle, définie par les fractions P_i/Q_i. On définit*

$$\Xi = \{Q_i(y)P_i(x) - P_i(y)Q_i(x)\} \subset \mathcal{F}(f(y))[\Theta_{\mathrm{ord}\, f}x].$$

Alors, f admet un inverse d'ordre r ssi la base standard réduite de l'idéal

$$\mathcal{J}_r = \left(\Theta_r\Xi\,;\left(\prod_{i=1}^{m} Q_i(x)\right) u - 1\right)_{\mathcal{F}(\Theta_r f(y))[\Theta_{r+\mathrm{ord}\, f}\, x,u]},$$

pour un ordre quelconque contient les polynômes $x_i - y_i$ $1 \leq i \leq n$.

PREUVE. Si f admet un inverse d'ordre r, alors en appliquant le lemme 1 p. 85, on voit que ces polynômes doivent appartenir à $\mathcal{J}_r$. D'autre part, ce même lemme montre que $\mathcal{J}_r \cap \mathcal{F}\langle y\rangle\{x\}$ est l'idéal $\Delta(g)$, où g désigne l'application rationnelle algébrique

$$g\colon (\Theta_{r+\mathrm{ord}\, f}\, x) \mapsto (\Theta_r f(y)).$$

On en déduit que $\mathcal{J}_r$ est premier et non trivial. Donc, pour tout i, $x_i - y_i$ appartient à la base standard réduite.

Réciproquement, si $x_i - y_i$ appartient à $\mathcal{J}_r$, alors $x_i \in \mathcal{F}(\Theta_r f(y))$ $i \in [1, r]$, d'après la prop. II.4.2.6, et donc f admet un inverse d'ordre r.

Remarque 3. — Ce résultat donne un autre moyen de tester l'existence pour f d'un inverse d'ordre r. Il suffit en effet de construire une base standard de l'idéal $[\Xi, (\prod_{i=1}^m Q_i(x))\, u-1]$, en tronquant les calculs à l'ordre $r + \mathrm{ord}\, f$. On peut aussi éviter de calculer une base standard réduite, et vérifier que le calcul de la base standard fait apparaître pour tout $1 \leq i \leq n$ un polynôme, dont le monôme de tête est x_i.

COROLLAIRE 1. — *Une application rationnelle différentielle $f\colon \mathbf{A}^n \mapsto \mathbf{A}^n$ est birrationnelle ssi la base standard réduite de l'idéal $\mathcal{J}_{n\,\mathrm{ord}\, f}$ contient pour tout i le polynôme $x_i - y_i$.* ∎

On va montrer qu'on peut majorer la complexité des calculs pour l'algorithme du th. 2, en se ramenant à la mise sous forme triangulaire d'une matrice, comme au chap. III § 2 n° 4. On prend cette fois l''idéal

$$\mathcal{J}_{r,i} = \left(\Theta_r\Xi\,;\left(\prod_{i=1}^{m} Q_i(x)\right)(x_i - y_i)\, u - 1\right)_{\mathcal{F}(\Theta_r f(y))[\Theta_{r+\mathrm{ord}\, f}\, x,u]},$$

Il faut alors tester que $\mathcal{J}_{r,i} = (1)$ $i \in [1, n]$.

Le nombre des variables est égal au nombre des dérivées de x d'ordre $r + \mathrm{ord}\, f$ au plus, augmenté de 1 pour la variable u. Donc, interviennent au plus $N = O\left((n)(r + \mathrm{ord}\, f)^m\right)$

variables. Le nullstellensatz effectif de KOLLÁR (cf. [Kol]) permet de borner le degré maximal des calculs intermédiaires par $d = (\deg f + 2)^N$. On a donc à trianguler un système linéaire de taille au plus $M \times LM$, où $M = O\left((\deg f)^{N^2}\right)$ est le nombre maximal de monômes et $L = (mO(r^m) + 1)$ le nombre maximal d'équations.

Les coefficients sont dans $\mathcal{F}\{y\}$, d'ordre $r + \operatorname{ord} f$ et de degré $\deg f$, au plus. Le nombre d'opérations élémentaires dans $\mathcal{F}\{y\}$ est polynômial en LM. Si l'on utilise la méthode de BAREISS, les coefficients intermédiaires sont des mineurs de la matrice, donc de degré borné par $D = M \deg f$ et de taille bornée par $S = O\left(D^N\right)$. Le coût d'une opération élémentaire dans $\mathcal{F}\{y\}$ en terme d'opérations élémentaires dans $\mathcal{F}$ est polynomial en S.

On en déduit le théorème suivant.

THÉORÈME 3. — *On peut tester qu'une application rationnelle différentielle $f\colon \mathbf{A}^n \mapsto \mathbf{A}^m$ admet un inverse d'ordre au plus r avec un coût, en terme d'opérations élémentaires sur $\mathcal{F}$ polynomial en*

$$O\left(L \deg(f)^{N^3}\right),$$

où $N = O((n)(r + \operatorname{ord} f)^m)$ et $L = (mO(r^m) + 1)$. ∎

COROLLAIRE 1. — *En particulier, cette borne s'applique pour tester qu'une application $f\colon \mathbf{A}^n \mapsto \mathbf{A}^n$ est birationnelle en prenant $r = n \operatorname{ord} f$ On a alors une complexité polynomiale en*

$$O\left(L \deg(f)^{N^3}\right),$$

où $N = O((n)((n+1)\operatorname{ord} f)^m)$ $L = (mO((n \operatorname{ord} f)^m) + 1)$. ∎

Remarques. — 4) Comme dans le cas algébrique, on ne peut pas utiliser pour prouver cette borne de complexité n'importe quel algorithme de base standard, car on ne pourrait pas contrôler la taille des coefficients.

5) On peut s'assurer que pour f d'ordre 0, on retrouve la borne donnée par le th. III.2.4.4 p. 52.

4. Relations avec le cadre général

Il faut prendre ici comme structure $\mathcal{A}$ la structure de $\mathcal{F}$-algèbre différentielle, pour $\mathcal{A}'$, celle de monoïde différentiel, pour $\mathcal{B}$ celle de module différentiel et pour $\mathcal{B}'$ celle de monomodule différentiel, correspondant à la définition suivante.

DÉFINITION 1. — *On appelle monomodule différentiel sur un monoïde différentiel A_Δ, un ensemble M avec une multiplication externe $A \times M \mapsto M$ et des dérivations $\delta : M \mapsto M$ $\delta \in \Delta$, commutant entre elles.*

Cette définition, strictement formelle, n'impose rien quant à la nature de ces applications. Un problème se pose : dispose-t-on d'un monomodule différentiel libre ? La réponse est heureusement oui. Pour tout ensemble E, il suffit de prendre l'ensemble $L \times E$, où L désigne le monoïde libre (non abélien) engendré par A et Δ, quotienté par la congruence identifiant $\delta\delta'$ et $\delta'\delta$ pour $(\delta, \delta') \in \Delta^2$, ainsi que aa' et $a'a$ pour $(a, a') \in A^2$. La manière de définir les opérations sur cet objet est évidente, de même que le fait qu'il satisfait bien la propriété voulue.

Si l'on applique la définition chap III § 1 n° 3 déf. 16., on trouve beaucoup plus de syzygies que dans la définition donnée ici. Il est aisé de voir que pour tout monôme m et tout polynôme P, il y a une syzygie (au sens du chap. III) de la forme : $(\delta(m\,P), \delta\,m\,P)$ ou de la forme $(\delta(m\,P), m\,\delta\,P)$. De telles syzygies sont trivialement réduites à 0 par P. Considérons un ensemble Σ de polynômes différentiels et notons par T l'ensemble des syzygies de cette forme pour tous les P de Σ, et par S l'ensemble des syzygies considérées dans ce paragraphe. On s'assure aisément que $T \cup S$ engendre l'ensemble total des syzygies entre éléments de $\mathbf{L}_\Sigma$, de sorte que S est bien un ensemble de syzygies essentielles au sens du chap. III § 1.

En fait ceci provient du fait que la définition des monomodules différentiels n'implique rien quand à la nature de “dérivations”, qui peuvent être absolument quelconques. Dans le cas particulier où elles reflètent l'action de dérivations sur les monômes de tête, $\delta(m_1 m_2)$ est égal à $\delta(m_1)m_2$ ou $m_1\delta(m_2)$, ce qui permet des simplifications. En revanche, le cadre général permet d'étendre la notion de base standard différentielle pour des opérateurs de dérivation quelconques : par exemple $\theta = (\delta_1^2 + \delta_2^2 - \delta_3^3)$. On pourrait alors construire des bases standard pour les idéaux stables par l'action de θ, mais il faut alors utiliser un ensemble de syzygies plus vaste, engendrant le monomodule différentiel des relations entre les monômes de tête pour l'opérateur θ.

Cette idée de se ramener à un ensemble de syzygies générateur est à la base de presque tous les critères pour éliminer les syzygies inutiles. Dans le cadre différentiel, une mise en œuvre efficace de ce principe resste à élaborer. Il faut en outre tenir compte du critère sur les monômes étrangers, qui semble d'une autre nature et typique de la structure d'idéal algébrique.

§ 2. ENSEMBLES CARACTÉRISTIQUES

1. Introduction

Les techniques d'algèbre différentielle utilisant des ensembles caractéristiques remontent aux travaux de RIQUIER, puis de JANET, étendus ensuite par RITT, KOLCHIN, etc. Elles ont été étudiées et utilisées par WU du point de vue des applications effectives, en particulier pour obtenir des algorithmes susceptibles de prouver des théorèmes de géométrie. On peut aussi trouver un exposé de méthodes constructives en algèbre différentielle, issues des résultats de Ritt, dans le livre de J. M. THOMAS, *Systems and Roots* ([Th]).

On aurait pu se dispenser d'un nouvel exposé de ces techniques si elles pouvaient permettre la détermination effective d'un ensemble caractéristique. Malheureusement, ce n'est pas le cas. Considérant un idéal $\mathcal{I} = [P_1, \ldots, P_p]$, on obtient seulement un ensemble autoréduit cohérent C tel que $[C] \subset \mathcal{I} \subset [C] : H_C$, où H_C^∞ désigne le produit des initiaux et séparants des polynômes de C. Il est fort possible que cet ensemble soit déjà un ensemble caractéristique, et c'est sans doute fréquemment le cas en pratique, mais on ne dispose pas de méthode générale pour le tester. RITT à montré comment on pouvait, en s'autorisant à factoriser, obtenir des ensembles caractéristiques $C_1, \ldots, C_k$ d'idéaux premiers $\mathcal{I}_1, \ldots, \mathcal{I}_k$ tel que $\{\mathcal{I}\} = \bigcap_{i=1}^{\ell} \mathcal{I}_{j_i}$.

Si l'on souhaite obtenir une méthode praticable, il est hautement préférable d'éviter autant que possible d'avoir à factoriser. D'autre part, même si l'on peut aboutir au résultat de l'algorithme de Ritt, bien des problèmes théoriques restent en suspens, par exemple on ne sait pas reconnaître les ensembles caractéristiques correspondant aux composantes de $\{\mathcal{I}\}$.

Pour les applications envisagées, on peut se limiter ici à considérer des idéaux premiers, mais on a absolument besoin d'un véritable ensemble caractéristique. On va donner une méthode permettant d'aboutir, si l'on a un moyen de tester l'appartenance à l'idéal premier considéré. Il peut sembler qu'on ne fait que déplacer le problème, mais par chance, dans les applications ultérieures à l'automatique, on se restreindra à des idéaux donnés par des équations d'état, ou de pseudo-état, qui forment déjà un ensemble caractéristique pour un ordre respectant l'ordre de dérivation.

On commence par introduire une notion de pseudo-base standard et l'on montre qu'elle coïncide avec celle d'ensemble caractéristique pour des idéaux premiers. Cette digression a seulement un intérêt conceptuel, faisant le lien entre deux approches voisines, mais sans apporter de contribution pratique notable sur le plan des méthodes. On donne ensuite un algorithme de construction, et des tests effectifs d'inversibilité d'applications rationnelles différentielles.

L'algorithme que l'on donne peut être rapproché de celui décrit par Daniel LAZARD dans son article [La], car les conditions qu'on impose à l'ensemble autoréduit et cohérent sont presque identiques. Toutefois, utilisant au maximum nos hypothèses, on peut en simplifier la mise en œuvre de manière à éviter les scindages, et le calcul dans des extensions "à la D^5" (cf. [DD] et [Du]).

2. Définitions

L'idée directrice est de considérer les ensembles caractéristiques comme des "pseudo-bases standard" avec une notion de réduction plus large et une filtration moins fine, c'est-à-dire ne satisfaisant pas la condition III.1.1.5 p. 43. Cette filtration provient d'un ordre admissible sur les dérivées, comme défini au chapitre I. Par la suite on supposera qu'un tel ordre $<$ a été choisi. $\mathcal{F}$ est un corps différentiel de caractéristique 0 et d'ensemble de dérivation $\Delta = \{\delta_1, \ldots, \delta_m\}$. On notera $\mathcal{R}$ l'anneau différentiel $\mathcal{F}\{x_1, \ldots, x_n\}$.

On rappelle qu'on note Υ l'ensemble $\Theta\{x_1, \ldots, x_n\}$, et $\deg P$ le degré de P en sa dérivée dominante v_P. On notera $x^d_{i,(\theta)}$ l'élément $(d, x_{i,(\theta)})$ de $\mathbf{N} \times \Upsilon$. On étend à cet ensemble les dérivations de Δ en posant $\delta\, x^d_{i,(\theta)} = x_{i,(\delta\theta)}$. L'ordre de Υ est étendu en posant $\upsilon^d < \nu^e$ si $\upsilon < \nu$ ou si $\upsilon = \nu$ et $d < e$. L'ensemble $\mathbf{N} \times \Upsilon$ est complété par un élément $\top$ tel que $\delta\top = \top\ \forall\delta \in \Delta$ et $\top > a\ \forall a \neq \top$, ainsi que d'un élément 1 tel que $\delta 1 = \top\ \forall\delta \in \Delta$ et $1 < a\ \forall a \neq 1$. On note $\mathcal{M}$ l'ensemble $\mathbf{N} \times \Upsilon \cup \{\top, 1\}$. On munit cet ensemble d'une structure de monoïde abélien en posant

A) $1a = a\ \forall a \in \mathcal{M}$,

B) $\upsilon^d \nu^e = \upsilon^d$ si $\upsilon > \nu$ et υ^{d+e} si $\upsilon = \nu$,

C) $a\top = \top\ \forall a \in \mathcal{M}$.

On a donc muni $\mathcal{M}$ d'une structure de monoïde différentiel ordonné.

On remarque que $\delta(a\, b) = \max(\delta\, a\, b, a\, \delta\, b)$.

On définit enfin une relation $\ll$ sur $\mathcal{M}$ par $\upsilon^d \ll \nu^e$ si $\upsilon < \nu$, $1 \ll a$ si $a \neq 1$ et $a \ll \top$ si $a \neq \top$.

DÉFINITION 1. — *On munit $\mathcal{M}$ d'une structure M de monomodule différentiel sur lui-même différente de la structure canonique en posant $a *_M b = a *_{\mathcal{M}} b$ si $b \not\ll a$ et $\top$ sinon.*

C'est cette structure qui sera considérée par la suite.

DÉFINITION 2. — *Soit $\mathcal{I}$ un idéal différentiel de $\mathcal{F}\{x_1, \ldots, x_n\}$, on définit une application τ de $\mathcal{I}$ dans M qui à un polynôme $P \in \mathcal{I} \setminus \mathcal{F}$ associe $\upsilon_P^{\deg P}$ si $I_P \notin \mathcal{I}$ et $\top$ sinon, $\top$ à 0 et 1 à tout polynôme non nul de $\mathcal{I} \cap \mathcal{F}$.*

Pour tout élément de $\mathcal{F}\{x_1, \ldots, x_n\}$, on appellera rang de P l'élément de $\mathcal{M}$ égal à $\top$ si $P = 0$, 1 si $P \in \mathcal{F}^*$, et $\upsilon_P^{\deg P}$ sinon.

PROPOSITION 1. — *Pour tout idéal différentiel $\mathcal{I}$ de $\mathcal{R}$, $\tau\mathcal{I}$ est un sous-monomodule différentiel de M.*

PREUVE. Si $\mathcal{I} = \mathcal{R}$, $\tau\mathcal{I} = \{1, \top\}$, qui est bien un sous-monomodule différentiel de M, puisque 1 est minimal et donc $a\,1 = \top$ dans M si $a \neq 1$. Autrement, soit a un élément de $\tau\mathcal{I}$. Il faut montrer que $\delta\, a \in \tau\mathcal{I}\ \forall \delta \in \Delta$. Si $a = \top$, ou si $a = \tau\, P$ et $S_P \notin \mathcal{I}$, c'est immédiat. Or, si $a \neq \top$, $I_P \notin \mathcal{I}$. Donc, si $\deg P = 1$, $S_P = I_P$ et $\delta\, a = \tau\, \delta\, a$. Supposons que $\deg P > 1$ et $S_P \in \mathcal{I}$, on a $I_{S_P} = \deg P\, I_P$, $\delta\tau\, S_P = \delta\tau\, P = \delta\, a$ et $\deg S_P = \deg P - 1$. Par récurrence, on se ramène au cas où $\deg P = 1$.

Reste à montrer que $ba \in \tau\mathcal{I}\ \forall b \in \mathcal{M}$. Si a ou b est $\top$ ou 1 c'est immédiat, de même que si $a \ll b$ ou $b \ll a$. Autrement, $a = \tau\, P$ avec $I_P \notin \mathcal{I}$ et $b = \upsilon_P^e$. Donc $\tau(\upsilon_P^e P) = ba$ puisque ce polynôme a même initial que P. ∎

DÉFINITION 3. — *On dit qu'un sous-ensemble C de $\mathcal{I}$ est une pseudo-base standard de $\mathcal{I}$ si le sous-monoïde différentiel de $\mathcal{M}$ engendré par $\tau C \cup \{\top\}$ est égal au sous-monoïde différentiel engendré par $\tau\mathcal{I}$.*

On a déjà introduit la notion de réduction au chapitre I. On en donne une seconde définition, équivalente, plus conforme à cette nouvelle approche.

DÉFINITION 4. — *Soit P un polynôme de $\mathcal{R}$, le reste de P est le polynôme $P - I_P\upsilon_P^{\deg P}$ si $P \notin \mathcal{F}$ et 0 sinon.*

On dit qu'un polynôme $P \in \mathcal{R}$ est réductible par un polynôme $Q \in \mathcal{R}$ si $P \neq 0$ et si $\operatorname{rg} P$ appartient au monomodule différentiel engendré par $\operatorname{rg} Q$, ou I_P est réductible par Q, ou reste P *est réductible par Q.*

On dit que P est élémentairement reduit à R par Q avec un facteur $I_{\theta\, Q}$, si $\operatorname{rg} P = \theta \operatorname{rg} Q$, et $R = I_{\theta\, Q} P - I_P \theta\, Q$, ou si I_P est élémentairement reduit à R_2 par Q avec un facteur F et $R = R_2 \upsilon_P^{\deg_P} + F \operatorname{reste} P$, ou enfin si reste P *est élémentairement réduit à R_2 par Q avec un facteur F, et $R = F I_P \upsilon_P^{\deg_P} + R_2$. On notera $P \xrightarrow{Q} R$. On notera $P \xrightarrow{Q^*} R$ la clôture transitive de cette relation.*

On peut décrire une procédure de réduction de la manière suivante. Chaque pas de réduction implique la multiplication par l'initial ou le séparant de Q. Il faut donc conserver en mémoire le facteur introduit. On peut pour cela utiliser une structure de tableau dont le premier élément est le polynôme à réduire et le second le facteur.

ALGORITHME 1.

---

réduction(P, Q) == réduction1$([P, 1], Q)$
réduction1(Rec, Q) ==
  $Q \in \mathcal{F}^* \Rightarrow [0, 1]$
  $Q = 0 \Rightarrow Rec$
  $P := Rec.pol$
  $\mathrm{rg}\, P < \mathrm{rg}\, Q$ ou $P = 0 \Rightarrow Rec$
  $\upsilon_P = \upsilon_Q \Rightarrow$
    réduction1$([I_Q P - I_P \upsilon_P^{\deg Q - \deg P} Q, I_Q Rec.fact], Q)$
  $\upsilon_P = \theta\, \upsilon_Q \Rightarrow$
    réduction1$([S_Q P - I_P \upsilon_P^{\deg Q - 1} \theta\, Q, I_Q Rec.fact], Q)$
  $Rec1 :=$ réduction1$([I_P, 1], Q)$; $Rec2 :=$ réduction1$([Rec1.fact \,\mathrm{reste}\, P, 1], Q)$
  $Rec3 := [Rec2.fact\; Rec1.pol + \; Rec2.pol, Rec2.fact\; Rec1.fact\; Rec.fact]$
  if $Rec3 = Rec$ then Rec else Reduction1$(Rec3, Q)$

C'est la manière dont j'ai implanté une procédure de réduction en Scratchpad II dans le cas différentiel ordinaire. La preuve de cet algorithme est aisée, et correspond exactement aux méthodes données par Ritt et Kolchin. On en déduit aisément un algorithme de réduction par rapport à un ensemble fini de polynômes

Lemme 1. — Un polynôme P est réduit à 0 par C ssi il existe un produit de puissances H des initiaux et séparants des polynômes de C, des monômes M_i et des opérateurs de dérivation θ_i tels que $HP = \sum_{i=1}^{k} M_i \theta_i Q_i$ où les Q_i sont des éléments de C, $\mathrm{rg} H \ll \mathrm{rg} P$ et $\mathrm{rg}(M_i \theta_i Q_i) > \mathrm{rg}(M_j \theta_j Q_j)$ $i < j$ ∎

DÉFINITION 5. — *On dira qu'une pseudo-base standard C de $\mathcal{I}$ est réduite si tout polynôme P de C est réduit par rapport à $C \setminus P$.*

THÉORÈME 1. — *Soit $\mathcal{I}$ un idéal différentiel premier de $\mathcal{R}$ et C un sous-ensemble de $\mathcal{R}$. Les propositions suivantes sont équivalentes :*
i) C est une pseudo-base standard réduite de $\mathcal{I}$
ii) C est autoréduit et tout les éléments de $\mathcal{I}$ sont réduits à 0 par C.
iii) C est un ensemble caracte'ristique de $\mathcal{I}$

PREUVE. *i)* $\Longrightarrow$ *ii)* Il suffit de prouver que tous les éléments de $\mathcal{I}$ sont réduits à 0 par C. Raisonnons par l'absurde. Soit P un polynôme de rang minimal qui ne puisse pas être réduit à 0 par C. Si $\tau\, P \neq \top$, P peut être élémentairement réduit par un polynôme de C en un polynôme de $\mathcal{I}$ de rang inférieur, qui doit donc être réduit à 0. Si $\tau\, P = \top$, $I_P \in \mathcal{I}$, donc I_P est réduit à 0 par C, ce qui implique que P peut être réduit en un polynôme de $\mathcal{I}$ de rang inférieur, et donc que P est réduit à 0 par C, contredisant l'hypothèse.

ii) $\Longrightarrow$ *iii)* Comme C est autoréduit, les initiaux des polynômes de C sont irréductibles par C, donc n'appartiennent pas à $\mathcal{I}$. Remarquant que $I_{S_P} \deg P\, I_P$, ceci implique que les séparants des polynômes de C ne sont pas réduits à 0 par C et n'appartiennent pas non plus à $\mathcal{I}$. Comme C réduit à 0 tous les polynômes de $\mathcal{I}$, $\mathcal{I} = [C] : H^\infty$, en notant H le produit de initiaux et séparants des polynômes de C.

Notons $\mathcal{J}$ l'idéal $(C)_{\mathcal{F}[y]} : H^\infty$, où y désigne l'ensemble des dérivées intervenant dans les polynômes de C. Tout élément de $\mathcal{J}$ est réduit à 0 par C, car il est dans $\mathcal{I}$. Montrons que $\mathcal{J}$ est premier. Si $PQ \in \mathcal{J}$, P ou Q appartiennent à $\mathcal{I}$. Ils sont donc l'un ou l'autre réduits à 0 par C, mais comme ils ne contiennent pas de dérivée propre des dérivées dominantes des polynômes de C, ceci implique que P ou Q appartiennent à $\mathcal{J}$. En dernier lieu, les S-polynômes associés aux pseudo-syzygies entre éléments de C, appartiennent à $\mathcal{I}$, donc sont réduits à 0 par C qui est donc cohérent. On peut donc appliquer la prop. I.4.1.6 p. 17, et conclure que C est un ensemble caractéristique de $\mathcal{I}$.

iii) $\Longrightarrow$ *i)* Si C est un ensemble caractéristique de $\mathcal{I}$, tout élément P de $\mathcal{I}$ est réduit à 0 par C. On en déduit que si $\tau P \neq \top$, il existe Q dans C tel que $\mathrm{rg}P = \upsilon_P^d \theta \mathrm{rg}Q$, puisqu'alors $I_P \notin \mathcal{I}$, ce qui implique d'après la proposition I.4.1.5 p. 17, $\mathcal{I}$ étant premier, que I_P n'est pas réduit à 0 par C. On en déduit que $\tau C = \mathrm{rg}C$ engendre $\tau\mathcal{I}$. ■

Remarque 1. — Si $\mathcal{I}$ n'est pas premier il peut ne pas admettre de pseudo-base standard réduite. Il suffit de considérer $[x^2, x'y]_{\mathbf{Q}\{x,y\}}$.

Concluons en définissant quelques ordres admissibles sur Υ.

DÉFINITION 6. — *On dit qu'un ordre admissible sur Υ élimine les variables $x_1, \ldots, x_i$ si $j \leq i < k$ implique $x_{j,(\theta)} > x_{k,(\theta')}$ $\forall(\theta, \theta') \in \Theta^2$.*

DÉFINITION 7. — *On appelle ordre d'élimination de $x_1, \ldots, x_i$ sur Υ l'ordre défini en posant $x_{j,(\theta)} > x_{k,(\theta')}$ si $j \leq i < k$ et en raffinant ensuite par l'ordre de la déf. I.4.1.3 p 15.*

Il est immédiat que cet ordre élimine bien les variables voulues. On peut aussi être plus brutal.

DÉFINITION 8. — *Ayant choisi un ordre sur Θ, par exemple l'ordre par ordre de dérivation puis lexicographique inverse ou l'ordre lexicographique pur, on appelle ordre par variables sur Υ l'ordre défini en posant $x_{i,(\theta)} \leq x_{j,(\theta')}$ si $i > j$ ou si $i = j$ et $\theta \leq \theta'$.*

3. Caractérisation. Procédure de complétion

DÉFINITION 9. — *Le rang d'une pseudo-syzygie (M, N) est le rang commun de M et N. On notera H_C le produit des initiaux et séparants de C, et υ_C l'ensemble des dérivées intervenant dans les polynômes de C.*

Lemme 2. — *Soit $C = \{f_1, \ldots, f_q\}$ un sous-ensemble autoréduit et cohérent de $\mathcal{R}$, avec $\upsilon_{f_i} < \upsilon_{f_j}$ $i < j$. On pose $\upsilon_C = \{x_1, \ldots, x_p, y_1, \ldots, y_q\}$, où les y_i sont les dérivées dominantes des polynômes de C, classées par ordre croissant, et $C' = \{f_1, \ldots, f_{q-1}\}$. On notera f'_q le polynôme f_q considéré comme un polynôme de $\mathrm{Fr}(\mathcal{F}[x_1, \ldots, x_n, y_1, \ldots, y_{q-1}]/\mathcal{J}')[y_i]$.*

Alors, C est un ensemble caractéristique d'un idéal premier $\mathcal{I}$ de $\mathcal{R}$ ssi pour tout l'idéal $\mathcal{J}' = (C') : H_{C'}$ est premier, et f'_q est premier et de degré égal à $\deg f_q$.

PREUVE. ($\Longrightarrow$) Si C est un ensemble caractéristique d'un idéal premier, $\mathcal{J} = (C) : H_C^\infty$ est premier d'après la prop. I.4.1.6 p. 17. Soit $\eta_1, \ldots, \eta_p, \epsilon_1, \ldots, \epsilon_q$ un zéro générique de $\mathcal{J}$. Posons $f'_q = \prod_{j=1}^{\ell} g_j$, où ϵ_1 est un zéro de $g_1(e_1, \ldots, e_t ap, \epsilon_1, \ldots, \epsilon_{q-1}, y_q$. Chassant les dénominateurs dans g_i, on obtient un polynôme P qui annule un zéro générique de $\mathcal{J}$, et qui appartient donc à $\mathcal{J}$. Il en résulte que P est réductible par C. Après réduction éventuelle, on peut supposer que P est réduit par rapport à $\{f_1, \ldots, f_{q-1}\}$, mais il ne peut pas être réduit à 0 car $I_P \notin \mathcal{J}$. Donc, si P est réductible, $\deg P = \deg f_q$. On en déduit que g_1 n'est pas un facteur propre de f_q.

($\Longleftarrow$) Utilisant encore la prop. I.4.1.6 p. 17, il faut montrer que $\mathcal{J} = (C) : H_C^\infty$ est premier et que le seul élément de $\mathcal{J}$ réduit par rapport à C est 0. Comme f'_q est de degré égal à $\deg f_q$, tout zéro générique de $\mathcal{J}'$ peut être complété en un zéro de $\mathcal{J}$: donc $\mathcal{J}' = \mathcal{J} \cap \mathcal{F}[x_1, \ldots, x_p, y_1, \ldots, y_{q-1}]$. Soit $(\eta_1, \ldots, \eta_{p+q-1}, \epsilon)$ un zéro générique d'une composante de $\{\mathcal{J}\}$. Le polynôme minimal de ϵ sur $\mathcal{F}(\eta)$ divise $f(\eta, y)$. Comme $f_q(\eta, y)$ est premier par hypothèse, ces polynômes coïncident à un facteur près, ce qui implique que $\{\mathcal{J}\}$ n'a qu'une composante. On en déduit que $\{\mathcal{J}\}$ est premier.

Soit maintenant un polynôme P de $\{\mathcal{J}\}$. Si $P \in \mathcal{J}'$, P est nul ou réductible par $\{f_1, \ldots, f_{q-1}\}$. Sinon, $P(\eta, y)$ est divisible par $f_q(\eta, y)$, donc P est réductible par C. Tous les polynômes de $\{J\}$ sont donc réduits à 0 par C, et appartiennent à $(C) :_{H_C}$ d'où l'on conclut aussi que $\mathcal{J} = \{\mathcal{J}\}$ est premier. ∎

Remarque 1. — On peut utiliser récursivement ce lemme, pour tester qu'un ensemble autoréduit et cohérent est bien un ensemble caractéristique d'un idéal. Cependant ceci nécessite de factoriser dans une tour d'extension algébrique, sauf cas particulier : par exemple si les polynômes sont trivialement absolument premiers. En particulier, on retrouve le fait qu'un idéal engendré par un système d'équations d'état ou de pseudo-état est premier, et que ce système est un ensemble caractéristique pour un ordre qui respecte l'ordre de dérivation.

Ce lemme, ainsi que la prop. I.4.1.6 p. 17, jouent un rôle crucial dans l'approche développée par Ritt et étendue par Kolchin. Nous allons avoir besoin d'un résultat légèrement différent, qui permet d'éviter un test impliquant des factorisations sur une tour d'extensions algébriques et l'hypothèse de réductibilité des éléments de $\mathcal{J}$ par C, loin de pouvoir être testée de manière effective.

THÉORÈME 2. — *Soient $\mathcal{I} = [\Sigma]$ un idéal premier non trivial de $\mathcal{R}$, $C = \{f_1, \ldots, f_q\}$, où les f_i sont rangés par rang croissant, un sous-ensemble autoréduit et cohérent de $\mathcal{I}$. On note C_i l'ensemble $\{f_1, \ldots, f_i\}$, C_0 sera $\{0\}$ par convention. On note à nouveau $x_1, \ldots, x_p$ les dérivées intervenant dans les polynômes f_i, mais qui ne sont pas la dérivée dominante d'un des f_i et $y_1, \ldots, y_q$, les dérivées dominantes des f_i. L'idéal $\mathcal{J}_i$ sera l'idéal engendré par C_i dans l'anneau $A_i = \mathcal{F}(x_1, \ldots, x_p)[y_1, \ldots, y_i]$.*

Alors, C est l'ensemble caractéristique de $\mathcal{I}$ ssi les trois conditions suivantes sont satisfaites :

A) tous les polynômes de Σ sont réduits à 0 par C,

B) les initiaux et séparants des polynômes de C n'appartiennent pas à $\mathcal{I}$,

C) pour tout f_i de C, l'initial de f_i est inversible dans $A_{i-1}/\mathcal{J}_{i-1}$,

D) le discriminant de f_i, considéré comme un polynôme en sa dérivée dominante est inversible dans $\mathbf{A}_{i-1}/\mathcal{J}_{i-1}$.

PREUVE. L'implication directe est immédiate en utilisant le lemme précédent.

($\Longleftarrow$) Comme l'idéal est premier, que H_C n'appartient pas à $\mathcal{I}$ et que C réduit à 0 les générateurs de $\mathcal{I}$, $\mathcal{I} = [C] : H_C^\infty$.

On commence par montrer que $\mathcal{I} \cap \mathcal{F}[x_1, \ldots, x_p, y_1, \ldots, y_q]$ est égal à $\mathcal{J} = (C) : H_C^\infty$. Soit P un polynôme de $\mathcal{I} \cap \mathcal{F}[x_1, \ldots, x_p, y_1, \ldots, y_q]$. Si P est réductible par C, la réduction s'opère sans dériver, et l'on obtient $H_C^a P = \sum_{i=1}^q M_i f_i + R$, où R est irréductible par C. Utilisant alors [Ko2 chap. III § 8 lem. 5 p. 137], on sait que $R \in (C) : H_C^\infty$, d'où la conclusion. Donc $\mathcal{J}$ est premier.

Les conditions C) et D) impliquent que $\mathcal{I}_i : H_{C_i} = \mathcal{I}_i$. En effet, les initiaux sont inversibles dans $A_i/\mathcal{I}_i$ et si le discriminant de f_j est inversible, on en déduit que le séparant de f_j est inversible car le discriminant est le résultant de f_j et de S_{f_j}. Utilisant le lemme précédent, il suffit de montrer que pour tout $i \in [1, q]$, f_i considéré comme un polynôme de $(A_{i-1}/\mathcal{J}_{i-1})[y_i]$ est premier. Soit i le plus petit indice tel que cette propriété soit fausse. L'utilisation récursive du lemme montre que $(C_j) : H_{C_j}$ est premier, donc que $\mathcal{I}_j$ $0 \leq j < i$ est premier. Ceci implique que $A_j/\mathcal{I}_j$ $0lej < i$ est un corps. Soit g_i un facteur premier de f_i, ϵ_i un zéro générique de g_i sur $A_{i-1}/\mathcal{I}_{i-1}$. On va montrer qu'on peut prolonger $\eta_i = (x_1, \ldots, x_p,\, y_1, \ldots, y_{i-1},\, \epsilon_i)$ en un zéro de $C : H_C$.

On pose $\mathcal{J}'_{i-1} = \mathcal{J}_{i-1}$ et $\mathcal{J}'_\ell = \mathcal{J}'_{\ell-1} + (g_\ell)$ $i \leq \ell \leq q$, où g_ℓ est un facteur premier de f_ℓ considéré comme un polynôme de $(A_\ell/\mathcal{J}'_{\ell-1})[y_\ell]$, $\eta_\ell = (\eta_{\ell-1}, \epsilon_\ell)$, où ϵ_ℓ est un zéro générique de g_ℓ. On va montrer par récurrence que pour tout $i-1 \leq \ell \leq q$:

a) $\mathcal{J}'_\ell$ est maximal dans A_ℓ et definit une composante de $V(\mathcal{J}_\ell)$,

b) $\ell = q$, ou bien l'initial et le discriminant de $f_{\ell+1}$ n'appartiennent pas à $\mathcal{J}'_\ell$.

Pour $\ell = i-1$, ces conditions sont trivialement satisfaites. Supposons les conditions vraies pour ℓ et montrons qu'elles sont vraies pour $\ell+1$. la condition a) est satisfaite car d'après l'hypothèse de récurence, $\mathcal{J}_{ell}$ est maximal, et l'initial de $f_{\ell+1}$ n'appartient pas à $\mathcal{J}_\ell$. On peut donc trouver un facteur premier $g_{\ell+1}$ de f_ℓ considéré comme un polynôme de $A_\ell/\mathcal{J}'_\ell[y_\ell]$. La primalité de $g_{\ell+1}$ implique que $\mathcal{J}'_\ell$ est maximal. D'autre part, l'adhérence de $\eta_{\ell+1}$ est la variété définie par $\mathcal{J}'_{\ell+1}$, qui définit donc une composante de $V(\mathcal{J}_{\ell+1})$. Si $\ell+1 = q$ la condition b) est satisfaite. Sinon, supposons que l'initial de $f_{\ell+2}$ s'annule sur $\mathcal{J}'_{\ell+1}$. Il serait alors diviseur de 0 dans $A_{\ell+1}/\mathcal{J}_{\ell+1}$, ce qui est impossible car il est supposé inversible dans $A_{\ell+1}/\mathcal{J}_{\ell+1}$ qui est bien un anneau unitaire puisque $\{\mathcal{J}_{\ell+1}\}$ est non trivial.

Ceci implique que η_q est un zéro générique de $C : H_C^\infty$, puisque cet idéal est premier, et donc ϵ_i un zero générique de tous les facteurs de (f_i) dans $A_{i-1}/\mathcal{J}_{i-1}$. Comme f_i est sans carré, son discriminant étant inversible, f_i est premier. ∎

On peut en déduire une méthode de construction d'ensemble caractéristique pour un idéal premier $\mathcal{I}$ de type fini. dès lors qu'on dispose d'une méthode pour tester qu'un polynôme appartient à $\mathcal{I}$. Dans l'algorithme, on désigne ce test par $P \in \mathcal{I}$. La première étape consiste à construire un ensemble autoréduit et cohérent réduisant à zéro tous les générateurs. Ceci utilise la méthode classique de RITT, WU Wen-Tsün, etc. Pour simplifier, on se donne un algorithme de construction d'un sous-ensemble autoréduit minimal d'un ensemble fini donné, *autRed*, ainsi qu'un algorithme construisant la liste des S-polynômes *SPol*.

Lors de la dernière étape, il faut pouvoir tester qu'un polynôme $P \notin \mathcal{I}_i$ est inversible dans $A_i/\mathcal{I}_i$ et calculer un représentant de l'inverse. Si P n'est pas inversible, c'est que $\mathcal{I}_i$ n'est pas premier. L'algorithme retournera alors un couple (Q, R) tel que $QR \in \mathcal{I}_i$, $Q \notin \mathcal{I}_i$ et $R \notin \mathcal{I}_i$. Pour les besoins de l'algorithme, on se donne une fonction *subRes*(P, Q, x, i) qui retourne le sous-résultant r de degré i de P et Q en la variable x, ainsi que a et b tels que $r = aP + bQ$. Ce résultat est donné sous la forme d'un tableau à trois clefs r, a et b. On utilise la syntaxe de Scratchpad II, avec le typage pour savoir si l'inversion a ou non échoué. Si c'est le cas, le résultat aura le type *FR* pour fraction rationnelle, sinon le type $Rec := Record[fact1 : Pol, fact2 : Pol]$. La fonction prend deux arguments, le polynôme P et la liste des polynômes C_i, rangés par ordre croissant.

ALGORITHME 2.

---

inverse($P, lPol$) : Union(Pol, Rec) ==
  if $P \in \mathcal{F}(y_1, \ldots, y_p)$ then return $1/P$
  for $f \in$ reverse($lPol$) repeat
    if $\deg_{v_f}(P) \neq 0$ then
      tab :=subRes($P, f_i, v_f, 0$)
      if $tab.r \neq 0$ then return $tab.a$ inverse($tab.r, lPol$)
      else
        for $j \in \mathbf{N}$ repeat
          if subRes(P, f, v_f, j).$r \neq 0$ then leave
          else rec : Rec := $[P, subRes(P, f_i, v_f, j).a]$
        return rec

PREUVE. La preuve de cet algorithme est immédiate, pour plus de détails on pourra se reporter à [La p. 9] ∎

On peut maintenant aborder l'algorithme de construction d'un ensemble caractéristique. Toutefois, il nous manque encore une définition, en effet, on va construire un ensemble cractéristique *normalisé* , selon l'approche de D. LAZARD dans [La].

DÉFINITION 10. — *On dit qu'un ensemble caractéristique C d'un idéal différentiel $\mathcal{I}$ est normalisé si les initiaux des polynômes de C ne font pas intervenir les dérivées dominantes des polynômes de C.* ∎

ALGORITHME 3.

```
ensembleCaractéristique(lPol)
  L_1 := []; flag := true
  while flag repeat
    until L_1 = [] repeat
      L_1 := []
      ensCar :=autRed(lPol)
      for pol ∈ lPol repeat
        if (rest :=réduction(pol, ensCar)) ≠ 0 then L_1 :=cons(rest, L_1)
      for sp ∈SPol(ensCar) repeat
        if (rest := réduction(pol, ensCar)) ≠ 0 then L_1 :=cons(rest, L_1)
      lPol :=append(L_1, lPol)
    flag := false
    for P ∈ ensCar repeat
      if I_P ∈ 𝓘 then flag := true ; lPol := cons(I_P, lPol)
      if S_P ∈ 𝓘 then flag := true ; lPol := cons(S_P, lPol)
      if (inv := inverse(I_P, ensCar)) case Rec then
        flag := true
        if inv.fact1 ∈ 𝓘 then new := inv.fact1 else new := inv.fact2
        lPol := cons(new, lPol)
      if (inv := inverse(S_P, ensCar)) case Rec then
        flag := true
        if inv.fact1 ∈ 𝓘 then new := inv.fact1 else new := inv.fact2
        lPol := cons(new, lPol)
  ensCarNorm := []
  for P ∈ ensCar repeat
    inv := inverse(I_P, ensCar)
    ensCarNorm := cons(numer(inv)v_P^(deg P) + denom(inv)reste(P), ensCarNorm)
  ensCarNorm
```

PREUVE. Il est manifeste d'après le théorème que si la procédure s'arrête, la liste $ensCar$ est bien un ensemble caractéristique de $\mathcal{I}$. Or, on remarque qu'à chaque nouvelle passe l'ensemble $ensCar$ décroît en rang. Comme il n'existe pas de suite strictement décroissante d'ensembles autoréduits, la procédure s'arrête. La dernière manipulation utilise le calcul des inverses des initiaux pour rendre l'ensemble caractéristique normalisé. Les nouveaux polynômes sont toujours dans l'idéal, et leur rang n'est pas perturbé, de sorte qu'il s'agit toujours d'un ensemble autoréduit minimal, donc d'un ensemble caractéristique. ∎

On peut maintenant indiquer deux types d'idéaux premiers pour lesquels on dispose d'un test effectif d'appartenance. Le premier cas est celui où le système de générateurs est déjà un ensemble caractéristique pour un certain ordre. On peut alors calculer un ensemble caractéristique pour un ordre différent.

Le deuxième correspond à l'idéal Δ défini au chapitre II, pour lequel la proposition III.4.2.3 p. 35 permet de conclure, par une simple évaluation.

Remarques. — 2) En particulier, l'algorithme ci-dessus est valable dans le cas algébrique pur, qui n'est qu'un cas particulier du cas différentiel. Si l'idéal premier est donné par un système de générateurs quelconques, on peut en calculer une base standard pour un ordre arbitraire, qui permet de tester l'appartenance à l'idéal. Ceci signifie donc qu'on peut en calculer un ensemble caractéristique de manière effective.

L'intérêt peut en sembler réduit. Toutefois, il serait intéressant de comparer le temps de calcul d'un ensemble caractéristique, qui est dans ce cas triangulaire, connaissant une base standard pour l'ordre lexicographique inverse, par rapport à celui d'une base standard pour l'ordre lexicographique pur. On sait que la méthode de FAUGÈRE répond à ce problème de manière particulièrement efficace, mais elle n'est valable que pour les idéaux zéro-dimensionnels, d'autre par la notion d'ensemble caractéristique est plus lâche que celle de base standard et ne comporte jamais plus d'éléments que de variables.

3) Si l'idéal différentiel premier est isobare et de type fini, on sait tester l'appartenance par un calcul de base standard différentielle comme au § 1. On peut donc alors aussi calculer un ensemble caractéristique.

Cette méthode apparaît à la fois comme une généralisation au cas différentiel de la méthode décrite par D. LAZARD dans [La], et comme un cas particulier car les hypothèses spécifiques où l'on se place permettent des simplifications. En fait le problème central pour déterminer un ensemble caractéristique, même dans le cas différentiel, est bien de nature purement algébrique. La condition de normalisation introduite par Lazard permet de lever les ambiguïtés et devrait aboutir à une méthode générale incluant le cas différentiel.

4. Applications

THÉORÈME 3. — *On considère une variété algébrique $X \subset \mathbf{A}^n_{\mathcal{F}}$, où $\mathcal{F}$ désigne un corps différentiel, définie par un idéal premier $\mathcal{I}$ et une application rationnelle f de X dans $\mathbf{A}^m_{\mathcal{F}}$ définie par m fractions $f_i = P_i/Q_i$, considérées comme des éléments de $K(X)$. Soit $\mathcal{J}$ l'idéal*

$$[\mathcal{I}, Q_i(x)u_i - 1, Q_i(x)T_i - P_i(x)]_{k\{u,x,T\}}$$

et $\mathcal{A}$ un ensemble caractéristique de $\mathcal{J}$ pour un ordre qui élimine les u, puis élimine successivement $x_1, \ldots, x_n$, alors f est inversible ssi pour tout x_i $\mathcal{A}$ contient un polynôme de la forme $S_i(T)x_i - R_i(T)$.

D'autre part, $\mathcal{A} \cap \mathcal{F}\{T\}$ est un ensemble caractéristique de l'idéal définissant l'image de f.

PREUVE. La preuve de la première partie est exactement semblable à celle du th. III.2.1.2 p. 50 qui traite le cas algébrique pur en utilisant les bases standard. On sait en effet que des polynômes de cette forme doivent être dans l'idéal, et les conditions sur l'ordre font qu'ils ne peuvent être réduits que par des polynômes de l'ensemble caractéristique qui ont eux-même cette forme.

La dernière assertion est immédiate. ■

Remarques. — 1) Si $\mathcal{I}$ est donné par un ensemble caractéristique C pour l'ordre $<$, notons M le polynôme $Rx_{n+1}-1$, où R désigne le reste de la réduction de H_C par C. On se ramène à un problème équivalent en considérant l'idéal $\mathcal{I}' = [C, M]_{\mathcal{F}\{n+1\}}$. Manifestement, $\mathcal{I}'$ est premier et engendré par $C' = C \cup \{M\}$, qui est un ensemble caractéristique pour tout ordre étendant $<$ et tel que $x_{n+1} > x_{i,(\theta)}$ $\forall i < n+1$, puisque C' est alors manifestement cohérent et autoréduit, et que M est absolument irréductible ce qui permet d'appliquer le lemme 3.2 p. 94.

f induit une application rationnelle f' de $X' = V(\mathcal{I}')$ dans $\mathbf{A}^m$, et f admet un inverse à gauche rationnel ssi f' en admet un. Sans restriction de généralité, on peut supposer que les polynômes $Q_iT_i - P_i$ sont réduits par rapport à C'. Si ce n'est pas le cas, on s'y ramène par l'algorithme de réduction, ce qui ne change pas la forme de ces polynômes ni le fait que les P_i/Q_i définissent f'. Q_iu_i est aussi réduit par rapport à C. Ces polynômes sont également absolument irréductibles. Pour un ordre sur $\Theta\{u, x, T\}$ qui prolonge $<$ et élimine u, T, l'ensemble des générateurs de J est autoréduit et cohérent. Utilisant encore le lemme 3.2, cet ensemble est donc un ensemble caractéristique de J. On peut donc calculer un ensemble caractéristique de $\mathcal{J}$, par l'algorithme 3.3 p. 97, pour un ordre satisfaisant les hypothèses du théorème. On a donc une méthode effective pour tester l'inversibilité de f.

2) Le fait de supposer qu'on connaît un ensemble caractéristique de $\mathcal{I}$ est une restriction, mais elle est moins forte que si l'on supposait $\mathcal{I}$ donné par un système fini de générateurs dans la mesure où, en général, les idéaux différentiels ne sont pas de type fini.

D'autre part, il nous faut supposer que $\mathcal{I}$ est premier, et on ne peut en général le savoir qu'en appliquant le n° 3 lem. 2., après avoir trouvé un ensemble caractéristique. Fort heureusement pour les applications, les systèmes considérés en automatique sont souvent donnés par des équations d'état et sont donc premiers “par construction”.

THÉORÈME 4. — *Soit $g, f_1, \ldots, f_m$ des fractions de $\mathcal{G} = \mathrm{Fr}\mathcal{F}\{n\}/\mathcal{I}$, avec $f = P/Q$ et $f_i = P_i/Q_i$, $\mathcal{A}$ un ensemble caractéristique pour un ordre quelconque de l'idéal*

$$\mathcal{J} = [\mathcal{I}; \mathrm{ppcm}(Q_i(x))u - 1; Q_i(y)P_i(x) - P_i(y)Q_i(x)]_{\mathcal{F}\langle f\rangle\{u,x\}},$$

alors $g \in \mathcal{F}\langle f\rangle$ ssi $R(g) = Q(y)P(x) - P(y)Q(x)$ est réduit à 0 par $\mathcal{A}$.

PREUVE. On sait d'après la prop. II.4.2.5 p. 36 que $g \in \mathcal{F}(f)$, ssi le polynôme $R(g)$ est dans l'idéal $\mathcal{G}\mathcal{J}$. Manifestement, $\mathcal{A}$ est un ensemble caractéristique de $\mathcal{G}\mathcal{J}$. Donc, si $g \in \mathcal{F}(f)$, $R(g)$ doit être réduit par $\mathcal{A}$.

Réciproquement, si le polynôme est réduit, il est dans

$$(\mathcal{G}[\mathcal{A}]) : H_{\mathcal{A}}^{\infty} = \mathcal{G}[\mathcal{A}] : H_{\mathcal{A}}^{\infty} = \mathcal{G}\mathcal{J},$$

donc $g \in \mathcal{F}\langle f\rangle$. ■

On a de nouveau le corollaire immédiat suivant.

COROLLAIRE 1. — *Sous les mêmes hypothèses, f définit une application rationnelle inversible ssi un ensemble caractéristique de $\mathcal{J}$ est*

$$\{x_i - y_i; u_i - \frac{1}{Q_i(y)}\}.$$

Tout ensemble caractéristique contient alors des polynômes identiques à un facteur près.
■

Remarque 3. — Si $\mathcal{I}$ est donné par un ensemble caractéristique, on peut sans problème calculer dans $\mathrm{Fr}\mathcal{F}\{n\}/\mathcal{I}$, car on dispose par réduction d'un test d'égalité à 0. D'après la proposition II.4.2.3 p. 35, un élément R de $\mathcal{F}\langle f\rangle\{x,u\}$ est dans $\mathcal{J}$ ssi

$$R(y, \frac{1}{\mathrm{ppcm}(Q_i(y))}) = 0,$$

ce qui donne un test commode d'appartenance à $\mathcal{J}$. On peut alors utiliser l'algorithme 3.3 p. 97 pour calculer un ensemble caractéristique de $\mathcal{J}$.

TROISIÈME PARTIE

Applications

CHAPITRE V

Structures et identifiabilité

Utilisant les notations de [K2], on a noté ci-dessus par θ un opérateur différentiel. Mais il est habituel dans de nombreux articles de désigner par θ le vecteur des paramètres d'une structure. C'est l'emploi qui en sera fait au cours de ce chapitre.

§ 1. STRUCTURES ET MODÈLES

1. Processus réel

Avant d'introduire une notion abstraite de modèle, tentons d'expliciter certaines hypothèses faites a priori sur le processus réel que l'on veut décrire. On peut supposer qu'il s'agit d'un dispositif expérimental, par exemple un montage de verrerie réalisé par un chimiste et dans lequel réagissent différentes substances. L'état d'un tel système peut être décrit à un instant donné par certaines grandeurs physiques, telles que la concentration des différentes espèces dans une éprouvette ou sa température.

Il évolue au cours du temps selon une loi qui dépend d'une part de paramètres internes, qui sont des constantes physiques comme le volume d'un récipient ou une constante de vitesse ; d'autre part de l'action de l'expérimentateur qui peut à tout instant introduire certaines substances en quantités arbitraires, modifier la température ou la pression etc...

L'expérience se concrétise par une moisson de mesures, que l'on suppose réalisées continûment au cours du temps. Les valeurs mesurées dépendent de l'état du système, mais les grandeurs d'état ne sont pas nécessairement directement mesurables, ni les paramètres internes connus. En revanche, on suppose connue l'action de l'expérimentateur, sous forme d'une ou de plusieurs fonctions dépendant du temps.

La modélisation va nécessiter le choix d'un protocole expérimental définissant les actions possibles de l'expérimentateur et les mesures qui seront effectuées parmi celles qui sont théoriquement et matériellement réalisables. Ensuite, on proposera une loi d'évolution du système, ce qui suppose le choix de grandeurs d'état significatives, si possible en nombre fini, et de paramètres internes a priori connus ou inconnus. On a alors défini une *structure*.

Le problème est désormais de déterminer un ensemble de valeurs pour les paramètres internes, compatibles avec les mesures effectuées. Cette évaluation définit un *modèle*, permettant ensuite de prédire l'évolution du système et éventuellement de le commander. Une première approche considère le système comme une boite noire, cherchant à décrire son comportement entrée-sortie sans se soucier de savoir si le modèle choisi correspond bien à la réalité physique.

Une seconde approche consiste à vouloir identifier avec certitude *le* modèle correspondant au processus réel. Il importe alors de pouvoir déterminer un modèle unique en fonction de l'expérience. C'est ce point de vue qui sera adopté par la suite.

2. Une classe de modèles

Les modèles que l'on considère correspondent aux hypothèses décrites au n°1. On impose néanmoins quelques restrictions quant à la forme mathématique de la loi décrivant le processus.

DÉFINITION 1. — *On appellera modèle paramétré, ou structure, sur un corps k, égal à $\mathbf{R}$ ou $\mathbf{C}$ la donnée d'entiers n, m, p et r, d'ensembles $D \subset k^r$ de paramètres admissibles, $E \subset k^n$ de vecteurs d'état admissibles, d'une classe d'applications $U \subset \mathrm{appl}(\mathbf{R}^+, k^m)$, de deux applications*

$$\begin{array}{lllll} f: & E \times D \times \mathbf{R}^+ \times k^m & \mapsto & E \\ g: & E \times D & \mapsto & k^p, \end{array}$$

et d'une famille d'applications

$$h_i : D :\mapsto k \ ; \ i \in I \subset \{1, \ldots, n\}.$$

On appellera système d'équations d'état du modèle paramétré le système

$$(1) \qquad \begin{array}{lll} dx/dt & = & f(x, \theta, t, u(t)) \\ y & = & g(x, \theta), \end{array}$$

et conditions initiales les équations du système

$$x_i(0) = h_i(\theta); \ \ i \in I,$$

où $t \in \mathbf{R}^+$ est le temps, $x \in E \subset k^n$ est le vecteur d'état, $y \in k^p$ est le vecteur d'observation et $\theta \in E \subset k^r$ est le vecteur des paramètres internes.

En donnant au vecteur des paramètres une valeur θ_0 particulière on obtient un modèle de la structure qui sera noté $M(\theta)$ si la structure est notée M.

Cette définition est conforme à l'idée intuitive qui a été développée, puisqu'on obtient un modèle du processus réel en fixant les valeurs des paramètres internes.

3. Structures particulières

Les structures linéaires auront par la suite un intérêt particulier, car on peut tester plus facilement par le calcul un certain nombre de leurs propriétés.

DÉFINITION 2. — *On appelle structure linéaire une structure pour laquelle le système d'équation d'état est de la forme*

$$(2)\qquad \begin{array}{lcl} dx/dt & = & A(t,\theta)x + B(t,\theta)u(t) \\ y & = & C(t,\theta)x, \end{array}$$

où A, B et C sont des matrices de tailles respectives $n \times n$, $n \times m$ et $p \times n$ dont les coefficients sont des fonctions du vecteur des paramètres θ et du temps t.

On dira qu'une structure est stationnaire si les fonctions f, g et h de la def. 2.1. sont indépendantes du temps, et qu'elle est polynomiale ou rationnelle si ces fonctions le sont. Enfin, on dira qu'elle est à conditions initiales nulles si les fonctions h_i définissant ces conditions sont nulles.

§ 2. COMPORTEMENT ENTRÉE-SORTIE

1. Définition

DÉFINITION 1. — *On appelle comportement entrée-sortie du modèle $M(\theta)$, défini en reprenant les notations de § 1, n° 1, déf. 1 l'application*

$$\begin{array}{cccc} \mathcal{C} & U & \mapsto & \mathrm{appl}(\mathbf{R}^+, \mathbf{R}^p) \\ & u & \mapsto & y. \end{array}$$

Le comportement entrée-sortie de la structure M est l'application $\mathcal{C}(\theta)$ qui à tout vecteur de paramètres θ de D associe le comportement entrée-sortie du modèle $M(\theta)$.

2. Résumés exhaustifs

Le comportement entrée-sortie d'une structure est un objet trop peu maniable pour être utilisé directement dans les applications, c'est pourquoi on cherche à lui substituer une fonction des paramètres internes plus simple, mais en un sens équivalente.

DÉFINITION 2. — *Soit M une structure, D son domaine de paramètres admissibles et $\mathcal{C}$ son comportement entrée-sortie, on appelle résumé (resp. résumé exhaustif), une application ρ de D dans un ensemble* E *telle que*

$$\forall(\theta,\theta') \in D^2 \mathcal{C}(\theta) = \mathcal{C}(\theta') \Longrightarrow \rho(\theta) = \rho(\theta')$$

$$(resp.)\qquad \forall(\theta,\theta') \in D^2 \mathcal{C}(\theta) = \mathcal{C}(\theta') \Longleftrightarrow \rho(\theta) = \rho(\theta').$$

Nous allons indiquer deux résumés exhaustifs bien connus, dans le cas des structures linéaires stationnaires avec conditions initiales nulles — on dira en abrégé *SLSCIN*.

DÉFINITION 3. — *On appelle paramètres de Markov d'une structure linéaire stationnaire définie en reprenant les notations de 1.3 déf. 2, les coefficients des matrices $CA^iB; i = 0, \ldots, 2n-1$*

DÉFINITION 4. — *On appelle matrice de transfert la matrice* $H(\lambda) = C(\lambda \mathrm{Id} - A)^{-1}B$ *où* Id *désigne la matrice identité.*

PROPOSITION 1. — *Les paramètres de Markov d'une structure SLSCIN forment un résumé exhaustif.*

PREUVE. Développant en série à l'origine les fonctions y_i pour une entrée analytique générique, on voit aisément que les matrices $CA^iB; i \in \mathbf{N}$ forment un résumé exhaustif. Le fait de pouvoir se restreindre à $i \leq 2n - 1$ provient du théorème de Caylley-Hamilton. ■

PROPOSITION 2. — *Considérant une SLSCIN et ayant mis les fractions de la matrice de transfert sous forme canonique, par exemple en chassant les facteurs communs et en rendant le coefficient principal du dénominateur égal à 1, les coefficients de* λ *dans le dénominateur et numérateur de toutes les fractions forment un résumé exhaustif.*

PREUVE. On trouve aisément ce résultat en considérant la transformée de Laplace de la sortie y. ■

§ 3. PROPRIÉTÉS DES MODÈLES

1. Identifiabilité

La présentation qu'on trouvera ici doit beaucoup au travaux de WALTER, LECOURTIER, RAKSANYI. Elle ne prétend pas à l'exhaustivité. En particulier, d'autres méthodes de test existent, qui ne sont pas évoquées ici. Pour une vue plus large du sujet, on se reportera à [Wa1], [Wa2], où à l'article de BELLMAN [Bel].

DÉFINITION 1. — *On dit qu'un modèle (resp. qu'une fonction* $\phi(\theta)$ *des paramètres d'un modèles)* $M(\theta)$ *d'une structure* M *est localement identifiable s'il existe un voisinage ouvert* $\mathcal{O}$ *de* θ*, dans le domaine des paramètres admissibles* D*, tel que*

$$\forall \theta' \in \mathcal{O}\ \mathcal{C}(\theta) = \mathcal{C}(\theta') \Longrightarrow \theta = \theta'$$

(resp.)
$$\forall \theta' \in \mathcal{O}\ \mathcal{C}(\theta) = \mathcal{C}(\theta') \Longrightarrow \phi(\theta) = \phi(\theta',)$$

où $\mathcal{C}(\theta)$ *désigne le comportement entrée-sortie de* $M(\theta)$*.*

DÉFINITION 2. — *Avec les mêmes notations que dans la définition précédente, on dit qu'un modèle (resp. qu'une fonction* $\phi(\theta)$ *des paramètres d'un modèle)* $M(\theta)$ *d'une structure* M *est globalement identifiable si*

$$\forall \theta' \in D\ \mathcal{C}(\theta) = \mathcal{C}(\theta') \Longrightarrow \theta = \theta'$$

(resp.)
$$\forall \theta' \in D\ \mathcal{C}(\theta) = \mathcal{C}(\theta') \Longrightarrow \phi(\theta) = \phi(\theta').$$

2. Discernabilité

Considérant deux structures en compétition pour décrire un même processus réel, il faut évidemment que les deux structures soient comparables, c'est-à-dire que commandes et mesures soient identiques. On se propose de savoir si l'expérience permettra de les départager. On se place naturellement dans un cadre idéalisé, où l'une des structures est supposée décrire la réalité.

DÉFINITION 3. — *Soient M et M' deux structures comparables et $M(\theta)$ un modèle de M. Notant $\mathcal{C}$, D et $\mathcal{C}'$, D' les comportements entrée-sortie et les ouverts de paramètres admissibles de M et M', on dit que $M(\theta)$ est discernable de M' si*

$$\forall \theta' \in D' \quad \mathcal{C}(\theta) \neq \mathcal{C}'(\theta').$$

Ceci signifie que si la structure M est la bonne et le modèle $M(\theta)$ le modèle correspondant à la réalité, alors on pourra déduire de l'expérience que la structure M' doit être rejetée, puisqu'elle ne pourra pas décrire le comportement entrée-sortie expérimental.

Le test de discernabilité est très semblable au test d'identifiabilité. Il a été aussi implanté en Scratchpad II. On a d'ailleurs la même borne de complexité en fonction du degré des résumés exhaustifs, mais expérimentalement l'identifiabilité se teste mieux. On aura l'ocasion de revenir sur ce sujet.

§ 4. PROPRIÉTÉS STRUCTURELLES

1. Définition

Cherchant à étendre une propriété des modèles aux structures, il est trop contraignant d'exiger que tous les modèles la satisfassent. En effet, avec cette définition, peu de structures intéressantes en pratique satisferaient les propriétés que nous venons de définir, même si celles-ci sont vérifiées par des modèles génériques. La définition suivante évite un tel inconvénient.

DÉFINITION 1. — *On dit qu'une propriété définie pour les modèles d'une structure M, est une propriété structurelle de M si elle est vérifiée par presque tous les modèles de la structure, au sens de la mesure uniforme sur $\mathbf{R}^q$.*

À titre d'illustration, considérons le cas de la discernabilité. Dire qu'une structure M est structurellement discernable d'une structure M' signifie que si la structure M est la bonne, l'expérience permettra presque sûrement d'écarter la structure M'. Mais il se peut qu'on ne puisse pas discerner M' de M.

2. Identifiabilité structurelle globale

Nous donnons une définition explicite de l'identifiabilité structurelle, conforme à la définition 1.1.

Définition 2. — *On dira qu'une structure M est structurellement globalement (resp. localement) identifiable s'il existe un sous-ensemble S de l'ensemble D des paramètres admissibles, de mesure nulle, tel que*

$$\forall\theta \in D \setminus S \; \forall\theta' \in D \; \mathcal{C}(\theta) = \mathcal{C}(\theta') \Longrightarrow \theta = \theta'$$

où $\mathcal{C}(\theta)$ désigne le comportement entrée-sortie de $M(\theta)$.

§ 5. LE PROBLÈME DE L'IDENTIFIABILITÉ

Dans ce dernier paragraphe, et pour toute la suite, nous ne considérerons plus que des structures admettant des résumés exhaustifs rationnels.

1. Transcription algébrique

Nous allons d'abord considérer le cas de l'identifiabilité structurelle locale.

Proposition 1. — *Soit M une structure admettant un résumé exhaustif rationnel $\rho : D \mapsto \mathbf{R}^r$ alors M est structurellement localement identifiable ssi le rang générique de la matrice jacobienne de ρ est égal à la dimension n de l'espace des paramètres.* ∎

Ceci peut être testé comme l'a fait Raksanyi par une méthode de triangularisation (cf [Ra]).

Corollaire 1. — *Sous les mêmes hypothèses, M est structurellement localement identifiable ssi le corps de fractions $k(\theta)$ est une extension algébrique de $k(\rho)$.* ∎

Remarques. — 1) On voit que l'identifiabilité structurelle locale est indépendante du domaine de paramètres admissibles choisis.

2) De plus, on voit que le caractère réel ou complexe de la structure ne joue aucun rôle.

En ce qui concerne l'identifiabilité structurelle globale, la situation est claire dans le cas où la structure est complexe et le domaine D égal à $\mathrm{Dom}(\rho)$. Dans ce cas, ayant obtenu un résumé exhaustif rationnel ρ, il faut tester que pour presque tout $\theta \in \mathbf{C}^m$, $\rho(\theta) = \rho(\theta')$ implique $\theta = \theta'$. Ceci revient à dire, puisque ρ est rationnelle, que ρ admet un inverse à gauche rationnel. Ceci peut être testé par les méthodes des chapitres III et IV. J'ai implanté en Scratchpad II la méthode du chap III § 2 n° 3 th. 3 cor. 1 p. 51.

Dans le cas réel, ou si $D \neq \mathrm{Dom}(\rho)$, le seul cas ambigu est celui où l'idéal $\mathcal{J}$, défini au th. III.2.3.1, est de dimension 0. Autrement, $k(\theta)$ n'est pas algébrique sur $k(\rho)$ et la structure n'est même pas structurellement localement identifiable. Une étude abstraite plus poussée pourrait être faite dans le cas réel si l'espace des paramètres admissibles est semi-algébrique, comme c'est en général le cas, par des méthodes de décomposition algébrique cylindrique, mais la complexité colossale des calculs laisse peu d'espoir (voir l'article de Fitchas, Galligo et Morgenstern [FGM]).

Le fait qu'il n'y ait qu'un nombre fini de solutions complexes possibles, explicitement connu car le calcul d'une base standard permet d'obtenir le degré de $\mathcal{J}$ et de pouvoir trancher après expérience. En effet, si l'on a pu déterminer une valeur possible pour θ, la résolution d'un système algébrique permet de les trouver toutes. On peut s'aider d'une base standard de $\mathcal{J}$ pour l'ordre lexicographique, ramenant à un système triangulaire et tester alors si les valeurs trouvées sont admissibles ou non. Il est d'ailleurs fort possible que des valeurs admissibles selon la définition abstraite de la structure puisse être rejetées si leur ordre de grandeur est inacceptable.

Il est plus efficace de calculer une base standard de $\mathcal{J}$ pour l'ordre lexicographique inverse et de passer ensuite à l'ordre lexicographique pur en utilisant le package de J. C. Faugère. On se reportera à l'article [FGLM] pour plus de détails.

On n'a donc pas de moyen efficace de répondre en toute rigueur à la question de l'identifiabilité, définie abstraitement, mais une transposition complexe permet d'obtenir une information substantielle, en général suffisante.

Un dernier problème concerne le corps de base. $\mathbf{C}$ ou $\mathbf{R}$ ne peuvent pas être représentés dans un système de calcul formel, mais en général les équations décrivant le système sont à coefficients rationnel. Si des grandeurs physiques devaient intervenir, on peut valablement les considérer comme génériques et donc transcendantes sur $\mathbf{Q}$ et travailler sur une extension transcendante pure de $\mathbf{Q}$. En particulier, si des considérations théoriques permettent de savoir que certains des paramètres θ_i sont identifiables, on peut les faire passer dans le corps de base, puisqu'ils sont supposés génériques.

Le problème qui demeure est de trouver des résumés exhaustifs rationnels. On sait en trouver dans le cas d'une structure SLSCIN rationnelle, qui sont même polynômiaux si la structure est polynomiale, comme il a été vu ci-dessus. D'autres méthodes existent pour certaines classes de structures non-linéaires, comme celle décrite par Vajda dans [Wa2 p. 42–48]. Le paragraphe suivant décrira une méthode s'appliquant à de nombreuses structures non-linéaires. Donnons d'abord quelques exemples dans le cas linéaire.

Exemples. — 1) Cet exemple provient de la thèse de Yves Lecourtier [Le p. 106–109]. On donne un exemple d'utilisation du package écrit en Scratchpad II, avec le résumé exhaustif provenant de la matrice de transfert.

La structure considérée décrit l'effet de premier passage d'un médicament, représenté par le diagramme suivant.

$$\begin{array}{ccccccc} u(t) & \to & (1) & \to & (2) & & \\ & & & \searrow & \downarrow & & \\ & & & & (3) & \to & \end{array}$$

Un médicament est absorbé en quantité $u(t)$. Il est présent dans le tube digestif en quantité x_1, et passe de là dans la circulation générale avec une vitesse $\theta_1 x_1$ où il est présent en quantité x_2. Il peut aussi passer dans la circulation générale en se dégradant en un métabolite, en quantité x_3, avec une vitesse $\theta_2 x_1$, ou se dégrader en métabolite après son passage avec une vitesse $\theta_3 x_2$. Le métabolite est évacué par voie urinaire à la vitesse $\theta_4 x_3$. Enfin, on observe les concentrations en médicament et métabolite, respectivement égales à $\theta_6 x_2$ et $\theta_7 x_3$. On prend comme domaines d'admissibilité pour les θ et les x les quadrants positifs de $\mathbf{R}^6$ et $\mathbf{R}^3$ respectivement — cet exemple est une simplification du cas où le médicament peut aussi être évacué avec une constante θ_5.

On veut savoir s'il est possible de définir les valeurs des paramètres θ. Voici un extrait d'une session Scratchpad II qui permet d'obtenir la réponse.

```
        (5)
            [- th2 - th1    0      0  ]    [1]
        dX  [                         ]    [ ]
        --= [    th1      - th3    0  ]X + [0]U
        dt  [                         ]    [ ]
            [    th2        th3   - th4]   [0]
            [0  th6   0 ]
        Y = [           ]X
            [0   0   th7]
        Paramètres internes = [th1,th2,th3,th4,th6,th7]
        Type: STRUCTLS
      identifiable?(struct,"Transfert")
        (6)  false
        Type: B      .06 (IN) + 3.584 (EV) + .027 (OT) = 3.0671 sec
```

Le résultat de type bouléen (B) est obtenu en un temps total de 0,33s.

On déduit aisément de la forme de la base standard calculée par le programme (voir appendice A), qu'une deuxième solution est donnée par :

$$
\begin{array}{rcl}
\theta'_1 & = & \theta_3 - \theta_2 \\
\theta'_2 & = & \theta_2 \\
\theta'_3 & = & \theta_1 + \theta_2 \\
\theta'_4 & = & \theta_4 \\
\theta'_6 & = & \theta_1\theta_6/(\theta_3 - \theta_2) \\
\theta'_7 & = & \theta_7.
\end{array}
$$

La réponse négative du programme peut donc être nuancée. D'une part les paramètres θ_2, θ_4 et θ_7 sont individuellement identifiables. D'autre part, si $\theta_3 > \theta_2$, la solution exédentaire est admissible, ce qui montre que la structure n'est pas structurellement globalement identifiable au sens de la définition formelle. En revanche, si l'on a trouvé un modèle solution avec $\theta_3 < \theta_2$, on sait que ce modèle est unique, donc globalement identifiable.

2) Cet exemple provient de [Ra p. 115–120]. On considère la structure linéaire stationnaire définie par les matrices :

$$
A = \begin{pmatrix}
-f_1(v_{3,1} + v_{2,1} + v_{0,1}) & f_1 v_{1,2} & f_1 v_{1,3} & 0 & 0 \\
f_2 v_{2,1} & -f_2(v_{3,2} + v_{2,1}) & f_2 v_{2,3} & 0 & 0 \\
f_3 v_{3,1} & f_3 v_{3,2} & -f_3(v_{4,3} + v_{2,3} + v_{1,3}) & f_3 v_{3,4} & 0 \\
0 & 0 & f_4 v_{4,3} & -f_4(v_{5,4} + v_{3,4}) & f_4 v_{4,5} \\
0 & 0 & 0 & f_5 v_{5,4} & -f_5(v_{4,5} + v_{0,5})
\end{pmatrix}
$$

$$
B = (0 \quad 0 \quad 0 \quad 0 \quad v)^T \quad C = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.
$$

Ce système décrit un modèle de synthèse de l'ammoniac, appartenant à une classe connue sous le nom de modèles de Horiuti ou de Temkin, et étudiés par John Appel.

$$
\begin{array}{ccccccccccc}
\leftarrow & N_2 & \rightleftharpoons & Nl & \rightleftharpoons & NHl & \rightleftharpoons & NH_2l & \rightleftharpoons & NH_3 \\
 & \downarrow & & & & & & & & \downarrow
\end{array}
$$

On se place dans un état chimiquement stationnaire, avec des débits d'hydrogène et d'azote constants. À l'instant $t = 0$, on commence à injecter une proportion $u(t)$ d'un isotope d'azote. Ceci a pour effet de rendre le modèle linéaire (cf [Wa1]). Les flèches indiquent les réactions élémentaires supposées permises. On mesure la concentration en isotope des produits sortants.

On associe à chacune des espèces présentes un compartiment, et l'on note x_i l'a quantité d'isotope dans le compartiment i à l'instant t, et f_i l'inverse de la quantité globale d'azote dans le compartiment. C'est une constante puisqu'on est dans un état stationnaire. À chaque flèche $(i) \to (j)$ correspond une constante de vitesse $v_{j,i}$ et à chaque flèche sortante $(i) \to$, une constante de vitesse $v_{0,i}$. Enfin v désigne le débit d'isotope à l'entrée.

$$\begin{array}{ccccccccccc} \leftarrow & (5) & \rightleftharpoons & (4) & \rightleftharpoons & (3) & \rightleftharpoons & (2) & \rightleftharpoons & (1) \\ & \downarrow & & & & & & & & \downarrow \end{array}$$

Dans cet exemple les résumés exhaustifs donnés ci-dessus sont d'une taille rédhibitoire. Mais Raksanyi a pu obtenir un résumé exhaustif d'une taille acceptable en utilisant les spécificités de la structure. Il a d'abord montré que certains paramètres peuvent s'exprimer linéairement à partir des précédents, car on est dans un état stationnaire :

$$\begin{aligned} v_{4,5} &= v_{0,1} + v_{5,4}, \\ v_{3,4} &= v_{4,3} + v_{0,1}, \\ v_{2,3} &= v_{3,2} + v_{0,1} + v_{3,1} - v_{1,3}, \\ v_{1,2} &= v_{0,1} + v_{2,1} + v_{3,1} - v_{1,3}, \\ v &= v_{0,1} + v_{0,5}. \end{aligned}$$

Les constantes $v_{0,1}$, $v_{0,5}$, f_1 et f_5 sont directement mesurables. D'autre part, il a pu prouver que les paramètres $v_{5,4}$, f_4, $v_{4,3}$ et f_3 sont structurellement globalement identifiables, en utilisant les propriétés des structures chaînées. Il ne reste donc plus à déterminer que les cinq paramètres $v_{1,3}$, $v_{2,1}$, $v_{3,1}$, $v_{3,2}$ et f_2.

On peut ensuite prouver que les coefficients des polynômes caractéristiques des sous-matrices principales d'ordre 2 et 3 de A forment un résumé exhaustif.

Le package IDPACK de Scratchpad prend 4 minutes sur IBM 4381 et 20 sec. environ sur un 3090 pour calculer une base standard permettant de conclure que cette structure n'est pas identifiable. Comme l'idéal est de dimension non nulle, il n'y a pas d'ambiguïté, puisqu'elle n'est même pas localement identifiable. On trouvera la session complète montrant la résolution de cette exemple à l'appendice A.

Raksanyi m'a fait savoir que sur cet exemple son algorithme de résolution échoue par manque de mémoire après près d'une journée de calcul. Même si l'on a eu recours à des ordinateurs puissants, le système d'exploitation est tel qu'on dispose en pratique de peu de mémoire (moins de 4 Mo). D'autre part, l'algorithme de base standard implanté en Scratchpad II est plutôt lent, comparé à des systèmes spécialisés comme Macaulay par exemple. Les raisons pour lesquelles ma méthode se comporte mieux sont difficiles à préciser. Notons que Raksanyi n'a pas utilisé le fait que l'idéal est premier, ce qui permettrait de simplifier et d'accélérer l'algorithme. Une implantation de la méthode du chapitre IV permettrait d'apprécier la valeur de cet argument. On peut surtout noter que si on a pu prouver une borne de complexité, en résolvant le système par les bases standard, la complexité de la méthode de Wu, et des méthodes voisines, est difficile à évaluer et encore très mal connue. Il n'est pas évident qu'elle soit plus rapide que l'algorithme de base standard, *avec l'ordre du degré*.

2. Discernabilité

Décrivons sommairement comment tester la discernabilité. Supposons qu'on ait deux stuctures comparables, M et M' admettant respectivement deux résumés exhaustifs rationnels ρ et ρ', définis par des fractions P_i/Q_i $i \in [1, q]$ et P'_i/Q'_i $i \in [1, q]$ et qui soient eux aussi comparables, c'est-à-dire tels que $M(\theta)$ et $M'(\theta')$ aient même comportement entrée-sortie ssi $\rho(\theta) = \rho'(\theta')$. Alors, pour tester que M_1 est discernable de M_2, il faut tester que l'idéal

$$\mathcal{I} = \left(\Big(\prod_{i=1}^{q} Q'_i(\theta')\Big) u - 1, P'_i(\theta') - P_i(\theta)/Q_i(\theta) Q_i(\theta') \right)_{k(\theta)[\theta', u]},$$

est égal à (1). Ceci peut être fait aisément par un algorithme de base standard et a donné lieu à une implantation en Scratchpad II. On se reportera à l'appendice A pour une démonstration et à l'appendice B § 1 pour le code source. Les paramètres de Markov donnent aisément des résumés exhaustifs comparables. On peut aussi utiliser la matrice de transfert (cf [Ra p. 109]). Cet idéal ressemble beaucoup à celui construit pour tester l'identifiabilité, et l'on a une borne de complexité du même ordre en utilisant le nullstellensatz effectif. Cependant, avec des résumés exhaustifs de taille comparable, le test d'identifiabilité est en général plus facile, phénomène qui reste à interpréter.

Bien entendu, comme pour l'identifiabilité, un résultat positif par cette méthode est absolument certain, tandis qu'un résultat négatif ne l'est que si le domaine des paramètres admissibles de M' est égal à $\mathbf{C}^{r'}$. Autrement, une discussion plus approfondie reste encore nécessaire. Théoriquement, la méthode de décomposition algébrique cylindrique permet de répondre de manière complète si l'espace des paramètres est semi-algébrique : mais on est sans doute encore loin de pouvoir l'appliquer sur de tels problèmes.

§ 6. STRUCTURES NON-LINÉAIRES

1. Structure avec conditions initiales génériques

On tente ici d'appliquer les résultats d'algèbre différentielle obtenus au cours des chapitres précédents, pour obtenir des résumés exhaustifs. L'utilisation de l'algèbre différentielle en automatique, pour laquelle M. Fliess a joué un rôle d'initiateur, est de nature à fournir à la fois un langage et des techniques de calcul appropriées, conjointement à l'emploi du calcul formel. On pourra se reporter à [Fl], ou à la thèse de Sette Diop [Di] pour une vue plus large de ces possibilités.

On considère une structure définie par un système d'équations d'état comme dans la déf. 1.2.1, où les fonctions f, g et h sont des polynômes ou des fractions rationnelles. Soit k, le corps engendré par les coefficients des équations définissant la structure, considéré comme un corps différentiel ordinaire avec une dérivation triviale. On prend comme corps de base le corps $\mathcal{F} = k\langle t, \theta, u\rangle$ où (t, θ, u) est une solution générique de l'idéal $[t' = 1, \theta'_i = 0]$ Le système d'équations d'état définit un idéal différentiel premier (cf. rem. IV.2.3.1 p. 94) $\mathcal{I}$ de dimension 0, et g une application rationnelle de $V(\mathcal{I})$ dans $\mathbf{A}^p$.

On se restreint à des structures satisfaisant les trois conditions suivantes.

A) La classe des commandes admissibles ne contient que des fonctions différentiellement transcendantes sur k [11], l'ensemble des paramètres admissibles ne contient que des constantes transcendantes sur k.

Remarque 1. — C'est une restriction que je n'ai pas su éviter, mais qui est acceptable d'un point de vue pratique. Les fonctions de commande ont, en pratique, peu de chance d'être exactement des solutions d'équations différentielles à coefficients constants, et la définition des propriétés structurelles suppose implicitement qu'on s'attend à trouver des valeurs génériques des paramètres.

On pourrait d'ailleurs généraliser en supposant u ou θ solutions génériques d'un idéal premier $\mathcal{J}$, *a priori connu*, pourvu qu'on ait un test effectif d'appartenance à $\mathcal{J}$, comme c'est le cas s'il est donné par un ensemble caratéristique ou une base standard finie — ce sera toujours le cas pour les paramètres puisqu'ils sont constants. Les développements sont aisés, mais je préfère laisser pour l'instant cette piste en suspens.

B) Pour u et θ génériques, l'unique solution du système d'état correspondant aux conditions initiales $x_i(0) = h_i(\theta)$ est générique.

Remarque 2. — C'est une condition plus restrictive, car il existe de mauvais cas. Par exemple, $x' = x,\ x(0) = 0$ définit la solution $x = 0$, qui n'est pas un zéro générique de $[x' - x]$. Cet exemple est trivial, mais on peut compliquer en prenant $x'' = x,\ x(0) = \theta,\ x'(0) = \theta$, dont la solution θe^t est un zéro générique de $[x' - x]$. En général, cette condition semble difficile à tester, mais elle est impliquée par la condition plus forte suivante, susceptible elle d'un test effectif.

B$'$) Les conditions initiales $h_i(\theta)$ sont telles que $K(h_i(\theta))$ est une extension transcendante pure de degré de transcendance n de K, où K désigne l'extension de k engendrée par les coefficients en θ intervenant dans les polynômes f et g.

Remarque 3. — Ceci est vrai en particulier si $h_i = \vartheta_i$ où les ϑ_i sont des paramètres tous distincts et n'intervenant pas dans les polynômes f_i et g_i.

C) Les fonctions mesures y ne sont pas singulières en $t = 0$, c'est à dire que si y_i est solution générique du polynôme $R(y)$, le séparant de ce polynôme ne s'annule pas en $t = 0$.

Remarque 4. — Il est vraisemblable que ce cas est peu fréquent et devrait être totalement exclus par des hypothèses raisonnables sur la structure, mais que je n'ai pas su définir. En tout état de cause, la régularité est facile à tester. D'autre part, il est manifeste que la condition B$'$) implique la condition C).

[11] Ceci n'exclut pas qu'il puisse ne pas y avoir d'entrée, on prend alors un ensemble de commandes vide.

Pour θ générique fixé, on sait que y est une solution générique de l'idéal $\mathcal{J}(\theta)$ définissant l'image de l'application rationnelle mesure g. Un ensemble caractéristique normalisé $\mathcal{A}(\theta)$ de cet idéal peut être obtenu en utilisant le graphe de g selon la technique décrite au chapitre IV § 2 n° 4 th. 3 p. 98. Comme $\mathcal{I}(\theta)$ est de dimension différentielle 0, $\mathcal{J}(\theta)$ est aussi de dimension différentielle 0. En effet, pour tout zéro générique η de $\mathcal{I}(\theta)$, $g(\eta)$ est un zéro générique de $\mathcal{J}$. Comme l'extension de corps engendrée par $g(\eta)$ est trivialement incluse dans celle engendrée par η, il suffit d'utiliser la prop. I.4.2.8. p. 19.

On en déduit que $\mathcal{A}(\theta)$ est de la forme $\{A(\theta)_1, \ldots, A(\theta)_p\}$ où $v_{A_i(\theta)} = y_{i,(e_i)}$. On peut obtenir de manière simple des conditions initiales $y_{i,(j)}(0) = H(\theta, u(0), u'(0), \ldots, u^{r_{i,j}}(0))$, pour i variant de 1 à n et j variant de 1 à e_i, en déterminant la valeur des dérivées successives des x_i en 0 à partir des équations d'état. Ces conditions initiales définissent y de manière unique, *pourvu que les séparants des polynômes* $A_i(\theta)$ *ne s'annulent pas en* 0. Ceci est toujours vrai sous les hypothèses de la condition B$'$), et plus généralement si y est régulière en 0. En effet, on peut alors calculer à partir de $\mathcal{A}$ et des conditions initiales le développement en série formelle de y.

L'application qui à θ associe le couple $(\mathcal{J}(\theta), H(\theta))$ est donc un résumé exhaustif du comportement entrée-sortie de la structure.

Les θ_i étant supposés génériques, la structure est structurellement globalement identifiable ssi cette application est injective. Reste à tester l'injectivité.

On note $\rho(\theta)$ le vecteur des coefficients en θ de tous les polynômes $H_i(\theta)$.

Remarque 5. — Cette notation n'est pas mensongère, puisqu'il s'agit bien d'un résumé, même s'il n'est pas exhaustif. On pourrait poursuivre le développement en série, ce qui donnerait un résumé exhaustif de taille infinie. Par noetherianité, on sait qu'on obtiendrait un résumé exhaustif fini, en tronquant ce développement à un certain ordre. Malheureusement, on ne sait pas en général déterminer cet ordre. Le but de la suite est de remédier à cet inconvénient.

On ne connaît pas directement $\mathcal{J}(\theta)$, mais on connaît $\mathcal{A}(\theta)$. Malheureusement, un ensemble caractéristique d'un idéal différentiel n'est pas unique en général. Cependant, on peut tester que deux ensembles caractéristiques définissent le même idéal par le lemme suivant, donné à titre d'exercice dans [Ko2 chap. IV § 9].

Lemme 1. — *Soient* $\mathcal{A}$ *et* $\mathcal{A}'$ *des ensembles caractéristiques des idéaux premiers* $\mathcal{I}$ *et* $\mathcal{I}'$ *de* $\mathcal{F}\{n\}$, *alors* $\mathcal{I}$ *est égal à* $\mathcal{I}'$ *ssi*

i) $H_{\mathcal{A}} \notin \mathcal{I}'$, $H_{\mathcal{A}'} \notin \mathcal{I}$, *en notant ainsi les produits des initiaux et séparants de* $\mathcal{A}$ *et* $\mathcal{A}'$,

ii) $\mathcal{A}$ *réduit à* 0 *tous les éléments de* $\mathcal{A}'$ *et* $\mathcal{A}'$ *réduit à* 0 *tous les éléments de* $\mathcal{A}$.

PREUVE. La condition est manifestement nécessaire. Si elle est vérifiée, on a $\mathcal{I} =\subset \mathcal{I}' = [\mathcal{A}'] : H_{\mathcal{A}'}^{\infty}$ puisque $\mathcal{A}'$ réduit à 0 tous les polynômes de $\mathcal{A}$ et $H_{\mathcal{A}'} \notin \mathcal{I}$. Par symétrie, on a l'inclusion inverse, d'où l'égalité. ■

Pour tous θ et θ', comme $\mathcal{A}(\theta)$ et $\mathcal{A}(\theta')$ ont même rang et que θ est supposé générique, il est manifeste que les initiaux et séparants de $\mathcal{A}(\theta)$ sont irréductibles et non nuls, donc qu'il n'appartiennent pas à $\mathcal{J}(\theta')$. L'égalité entre $\mathcal{J}(\theta)$ et $\mathcal{J}(\theta')$ est donc équivalente au fait que les polynômes de $\mathcal{A}(\theta)$ sont réduits à 0 par θ' et réciproquement. On pose $\mathcal{A}(\theta) = \{\mathcal{A}(\theta)_1, \ldots, \mathcal{A}(\theta)_\ell\}$. On effectue la réduction formelle de $\mathcal{A}(\theta)_i$ par $\mathcal{A}(\theta')$. On trouve un polynôme $R(\theta, \theta')_i$ dans $k\langle\theta, \theta', t, u\rangle[y]$, en général non nul et irréductible par

$\mathcal{A}(\theta')$. Chassant les dénominateurs, l'égalité à 0 est équivalente au fait que les coefficients $\varrho_{i,j}(\theta, \theta')$ sont tous nuls.

On peut maintenant utiliser le fait que $\mathcal{A}$ est supposée normalisée. En effet, ceci implique que l'initial de tout polynôme A de $\mathcal{A}$ ne contient aucune dérivée dominante d'un polynôme de $\mathcal{A}$. Pour réduite $A(\theta')$ par $\mathcal{A}(\theta)$, la première étape consiste nécessairement à le réduire en

$$I_{A(\theta)}A(\theta') - I_{A(\theta')}A(\theta),$$

qui est alors irréductible par $\mathcal{A}(\theta)$. On en déduit que

$$\frac{A(\theta)}{I_{A(\theta)}} = \frac{A(\theta')}{I_{A(\theta')}},$$

donc que $A(\theta)$ et $A(\theta')$ doivent coïncider à un coefficient près, d'où le théorème suivant.

THÉORÈME 1. — *Soit M une structure satisfaisant les conditions A), B), et C) et $\mathcal{A} = \{A_i\ i \in [1, n]\}$ un ensemble cractéristique normalisé de l'idéal $\mathcal{J}$ dont la sortie y est solution générique. On peut supposer que A_i appartient à l'anneau $k(\theta)\{y, t, u\}$, en chassant éventuellement les dénominateurs en u et t. Choisissons alors un ordre total sur les monômes de $k(\theta)\{y, t, u\}$, et en prenons $A_i(\theta)$ tel que son monôme dominant apparaisse avec coefficient 1.*

Sous ces hypothèses, les coefficients $\mu_{i,j}(\theta)$ apparaissant dans $A_i(\theta)$ sont tels que

$$\theta \mapsto (\mu_{i,j}(\theta), \rho(\theta)),$$

où ρ est le résumé donné par les conditions initiales, forme un résumé exhaustif de la structure M. ■

Remarque 6. — Pour toute structure, même si elle ne satisfait pas les conditions A) et B), on peut calculer un ensemble caractéristique normalisé $\mathcal{A}$ de l'idéal $\mathcal{J}$ et des conditions initiales H_i. Il suffit alors qu'elle vérifie la condition C), c'est-à-dire que séparants ne s'annulent pas quand on y substitue les conditions initiales, pour que la donnée de $\mathcal{A}$ et des H_i détermine la solution de manière unique. Ceci signifie qu'on peut de manière plus générale conclure à la non-identifiabilité. Car si $\rho(\theta) = \rho(\theta')$ et $\mu(\theta) = \mu(\theta')$ n'impliquent pas l'égalité de θ' et θ, la structure n'est certainement pas identifiable.

Donnons un exemple.

Exemples. — 1) Considérons la structure définie par

$$\begin{aligned}
x_1' &= -(\theta_1 + \theta_2)x_1 + (\theta_5 u + \theta_3)x_2,\\
x_2' &= \theta_2 x_1 - (\theta_3 + \theta_4)x_2,\\
y &= x_1,\\
x_1(0) &= \theta_6,\\
x_2(0) &= \theta_7,
\end{aligned}$$

qui provient de l'article [LLW], donnant des exemples de structures non linéaires et non identifiable non triviale dont l'existence était, faute d'exemples et surtout de technique pour tester la non identifiabilité, mise en doute au moment de sa publication. On a cependant modifié l'exemple, de manière à le faire entrer dans notre cadre, en rendant les conditions initiales génériques. Comme $y = x_1$, il suffit d'éliminer x_2 dans les deux premières équations. On prend donc un ordre tel que x_2 et toutes ses dérivées soit plus grand que x_1 et ses dérivées.

Réduisant la seconde équation par la dérivée de la première, on obtient

$$(-\theta_5 u' + (\theta_3+\theta_4)(\theta_5 u+\theta_3))x_2 + x_1'' + (\theta_1+\theta_2)x_1' - \theta_2(\theta_5 u+\theta_3)x_1.$$

Enfin, réduisant ce polynôme par la première équation, on trouve

$$\begin{aligned} P =&(\theta_5 u+\theta_3)x_1'' \\ &+ (-\theta_5 u' + \theta_5(\theta_1+\theta_2+\theta_3+\theta_4)u + \theta_3(\theta_1+\theta_2+\theta_3+\theta_4))x_1' \\ &+ (-\theta_5(\theta_1+\theta_2)u' - \theta_5^2\theta_2 u^2 + \theta_5((\theta_3+\theta_4)(\theta_1+\theta_2) - 2\theta_2\theta_3)u + (\theta_3+\theta_4)\theta_3(\theta_1+\theta_2) - \theta_2\theta_3^2)x_1, \end{aligned}$$

qui forme précisément un ensemble caractéristique normalisé de l'idéal premier définissant l'image — les conditions données au chapitre IV § 2 n° 3 th. 2 p. 94 sont trivialement satisfaites.

Les conditions initiales s'obtiennent facilement :

$$\begin{aligned} x_1(0) &= \theta_6 \\ x_1'(0) &= \theta_5\theta_7 u(0) - (\theta_1+\theta_2)\theta_6 + \theta_3\theta_7 \end{aligned}.$$

On peut donc appliquer le théorème 1 ci-dessus. Divisant par θ_5, on obtient un résumé exhaustif en prenant les coefficients de P, et les conditions initiales :

$$\begin{aligned} \theta_3/\theta_5, \\ \theta_1+\theta_2+\theta_3+\theta_4, \\ \theta_3(\theta_1+\theta_2+\theta_3+\theta_4)/\theta_5, \\ \theta_1+\theta_2, \\ \theta_5\theta_2, \\ (\theta_3+\theta_4)(\theta_1+\theta_2) - 2\theta_3\theta_2, \\ ((\theta_3+\theta_4)(\theta_1+\theta_2)\theta_3 - \theta_2\theta_3^2)/\theta_5, \\ \theta_6, \\ \theta_5\theta_7, \\ (\theta_1+\theta_2)\theta_6 + \theta_3\theta_7, \end{aligned}$$

d'où l'on déduit que la structure n'est pas identifiable, puisque les 3^e^, 6^e^, 7^e^ et 10^e^ équations sont impliquées par les autres. Il ne reste alors au plus que 6 conditions indépendantes pour 7 variables. Si l'on prend $\theta_6 = 1$ et $\theta_7 = 0$, on retrouve le modèle exact considéré dans l'article. Évaluant θ_6 et θ_7 dans le résumé exhaustif ci-dessus, on retrouve bien un système équivalent au résultat donné dans l'article. Comme le séparant de P ne s'annule pas en 0, même après cette substitution, on peut utiliser la remarque 6 ci-dessus et retrouver le résultat précis de l'article. En revanche, si la structure avait été identifiable, on n'aurait guère pu conclure qu'avec des conditions initiales génériques.

2) On va donner un exemple d'application à la discernabilité. Considérons la structure M définie par

$$\begin{aligned} P_1(x) = x'' + \theta_1 x' + \theta_2 x = 0, \\ x(0) = \theta_3, \\ x'(0) = \theta_4, \\ y = x, \end{aligned}$$

et la structure M' définie par

$$\begin{aligned} P_2(x) = x' + \vartheta_1 x = 0, \\ x(0) = \vartheta_2, \\ y = x. \end{aligned}$$

Il est manifeste que $\theta_1, \ldots, \theta_4$ forme un résumé exhaustif de M et $\vartheta_1, \ldots, \vartheta_2$ un résumé exhaustif de M'. Toutefois, ces résumés peuvent pas être comparés directement, car les ordres de P_1 et P_2 ne coïncident pas. Une condition nécessaire et suffisante pour que M puisse être discernée de M' est que y ne soit pas solution de $P'(y) = 0$ ou ne soit pas solution de $y(0) = \vartheta_2$. Ceci est manifeste, car l'ordre de P_2 est strictement inférieur à celui de P_1 et y est un zéro générique de P_1.

Réciproquement, pour tester si M' est discernable de M, on peut d'abord réduire $P_1(y)$ par $P_2(y)$, ce qui donne un reste

$$R(y) = (\vartheta_1^2 - \theta_1\vartheta_1 + theta_2)y,$$

qui doit être identiquement nul. D'autre part, on doit avoir

$$\begin{aligned} \vartheta_2 &= \theta_3, \\ -\vartheta_1\vartheta_2 &= \theta_4. \end{aligned}$$

Il est immédiat de voir que pour ϑ générique, ce système admet la solution

$$\begin{aligned} \theta_1 &= \vartheta_1, \\ \theta_2 &= 0, \\ \theta_4 &= \vartheta_1\vartheta_2, \\ \theta_3 &= \vartheta_2, \end{aligned}$$

Ce qui montre que M' est indiscernable de M.

La simplicité de cet exemple cache une difficulté majeure. En effet, on a pu raisonner de la sorte car les initiaux et séparants de P_1 et P_2 valent 1. Dans le cas général, on est amené à exprimer algébriquement l'inclusion de deux variétés algébriques différentielles. Or, à ma connaissance, on ignore comment tester algorithmiquement l'inclusion de deux variétés.

Exemple 3. — Considérons les variétés algébriques différentielles V_1, V_2 et V_3 qui sont les composantes générales des polynômes premiers $P_1 = (y')^2 - 4y$, $P_2 = (y')^2 - y^3$ et $P_3 = y$. La variété V_3 n'est pas incluse dans V_1, mais elle est incluse dans V_2. Cependant, P_3 réduit à 0 P_1 et P_2. L'ambiguïté vient du fait qu'il réduit aussi à 0 S_{P_1} et S_{P_2}. Dans un cas, $V(P_3)$ est une composante isolée de $V(P_1)$, distincte de sa composante générale, tandis que $V(P_2)$ n'a qu'une composante contenant $V(P_3)$. On se reportera à [Ri2 chap. III § 2] pour plus de détails.

2. Possibilités d'emploi et d'extension

On a pu donner ici une méthode, théoriquement utilisable pour toute structure générique. Deux problèmes se posent. Est-elle praticable ? Que faire si la structure n'est pas générique ?

En ce qui concerne le premier problème, on ne peut comparer que par rapport aux techniques existantes, applicables à tout coup sur une large classe de structure, donc principalement les méthodes calculant un résumé exhaustif par la matrice de transfert ou les paramètres de Markov dans le cas des SLSCIN. Or, précisément, notre technique a un champ d'application orthogonal à celui des méthodes précédentes, puisqu'elles supposent des conditions initiales nulles, alors qu'il nous faut des conditions génériques. Ceci n'interdit pas de comparer les performances relatives pour des structures linéaires de même taille.

Un certain nombre d'exemples me donnent l'espoir de pouvoir traiter des structures plus complexes qu'avec les résumés classiques.

Exemple 1. — Si l'on considère une structure linéaire telle que les matrices A et B soient génériques, et la matrice C égale à l'identité. Dans un tel cas, le calcul d'ensemble caractéristique consiste uniquement à substituer les y aux x. On retrouve alors un résultat bien connu : la structure est identifiable, et le coût des calculs est dérisoire.

En revanche, le calcul de la matrice de transfert ou des paramètres de Markov serait désastreux avec des matrices génériques pleines.

La portée d'un tel exemple est bien sûr très relative. Il montre cependant comment notre algorithme parvient à déjouer quelques pièges grossiers.

La question de la généricité pose d'autres problèmes. Il faudrait disposer d'un test effectif qui retourne, si la solution n'est pas générique, un idéal plus petit la définissant. On pourrait alors se ramener au cas générique et traiter potentiellement des exemples quelconques.

On peut enfin remarquer qu'on n'a aucune raison de se limiter à des structures polynomiales ou rationelles. Plus précisément, si les fonctions sont solutions d'équations différentielles simples, on peut se ramener au cas polynomial.

Exemple 2. — Considérons la structure :

$$\begin{aligned} x'' &= -\theta_1 \sin x + \theta_2 u, \\ y &= \cos(x), \\ x(0) &= \theta_3, \\ x'(0) &= \theta_4. \end{aligned}$$

Elle se ramène simplement à la structure équivalente :

$$\begin{aligned}
x_2' &= -x' x_3,\\
x_3^2 + x_2^2 &= 1,\\
x'' &= -\theta_1 x_3 + \theta_2 u,\\
y &= x_2,\\
x(0) &= \theta_3,\\
x'(0) &= \theta_4,\\
x_2(0) &= \cos(\theta_3),\\
x_3(0) &= \sin(\theta_3).
\end{aligned}$$

Les variables x_2 et x_3 représentent respectivement $\cos(x)$ et $\sin(x)$. Bien sûr, ceci ne peut qu'accroître le coût des opérations, mais une approximation n'est peut-être pas toujours suffisante, et peut surtout modifier les propriétés structurelles. Il est donc intéressant de savoir qu'on *pourrait* le faire, au moins dans certains cas. Ici, les calculs sont assez simples pour être traités à la main. On trouve que y est solution de

$$\begin{aligned}
P(y) &= (1-y^2)^2(y'')^2 + 2(y(y')^2 + \theta_1 y^2 - \theta_1)(1-y^2)y''\\
&\quad + y^2(y')^4 - 2\theta_1(1-y^2)y(y')^2 + \theta_1^2 y^8 \theta_2^2 u^2 y^6 + \cdots,\\
y(0) &= \cos(\theta_3),\\
y'(0) &= -\theta_4 \sin(\theta_3),\\
y''(0) &= \theta_1 \sin^2(\theta_3) - \theta_2 u(0)\sin(\theta_3) - \theta_4^2\cos(\theta_3),
\end{aligned}$$

où les coefficients de P sont fonctions de θ_1 et θ_2^2.

On peut se convaincre assez aisément que la structure est générique. Cependant, il faut être prudent, car cela n'aurait pas été le cas si l'on avait modélisé $\sin(x)$ et $\cos(x)$ en posant :

$$\begin{aligned}
x_2' &= -x' x_3,\\
x_3' &= x' x_2.
\end{aligned}$$

D'autre part, les calculs seraient devenus bien plus compliqués. À partir de la solution donnée, il est clair que θ_1, $|\theta_2|$, $|\theta_4|$, $\cos(\theta_3)$ et $|\sin(\theta_3)|$ sont structurellement globalement identifiables. En outre, on connaît le signe de $\theta_2\sin(\theta_3)$ et de $\theta_4\sin(\theta_3)$; il n'y a donc que deux solutions possibles pour θ_1, θ_2 et θ_4, ainsi que pour la valeur de θ_3 à 2π près.

Une difficulté théorique profonde limite tout de même les possibilités d'applications effectives. En effet, si le traitement du système d'équations différentielles est résolu de manière totalement algorithmique par la méthode du chap. IV § 2, la difficulté vient des conditions initiales, puisqu'on est conduit à résoudre un système non algébrique, hors de portée des méthodes algorithmiques actuelles, bien qu'il puisse être ici aisément traité à la main.

Conclusion

Au terme de ce travail, il paraît opportun de faire un bilan des résultats obtenus. Ceci revient en un sens à dresser la liste des questions ouvertes, des difficultés qui ont pu être contournées pour parvenir quand même aux buts fixés, parfois au prix d'une perte de généralité, tout en soulignant la portée des résultats obtenus. Un certain nombre de ces problèmes me paraissent dignes d'intérêt, par les possibilités nouvelles qu'apporterait leur résolution, tant sur le plan théorique que pratique.

1. Implantations. Problèmes algorithmiques

Des algorithmes décrits ici, seuls ont été implantés la méthode utilisant l'idéal Δ, et les manipulations de structures linéaires stationnaires, sans oublier un package de construction de base canonique. Une implantation de la procédure de construction de base standard différentielle, et de l'algorithme de construction d'ensemble caractéristique du chapitre IV sont indispensables pour se faire une idée précise des problèmes rencontrés dans leur mise en œuvre, de leur efficacité potentielle, et surtout pour traiter des exemples permettant de cerner les mauvais cas, d'épurer et de compléter les méthodes algorithmiques.

Au cours de mon travail d'implantation, j'ai rencontré les problèmes suivants.

A) En ce qui concerne les tests d'inversibilité, on a vu à travers des exemples que la méthode de l'idéal Δ, et celle utilisant les bases canoniques losrqu'elle s'applique, sont plus rapides que la méthode du graphe. Cependant, elle ne donnent pas l'expression de l'inverse qu'on peut néanmoins souhaiter connaître. C'est la rançon de l'efficacité, car la lenteur des calculs pour le graphe est sans doute très liée à la taille de l'inverse. Si l'on peut se passer d'une expression développée de l'inverse, la trace des calculs de base canonique est souvent de taille plus raisonnable et constitue un "programme de calcul de l'inverse" mieux adapté aux besoins pratiques. Mon implantation permet de conserver cette trace, mais des efforts restent à faire pour la rendre lisible et utilisable.

Dans le cas de l'idéal $\Delta(K)$, les coefficients des polynômes présents à chaque étape du calcul de la base standard engendrent le corps K, de sorte que ce corps est au même titre que l'idéal un des invariants de l'algorithme. La trace des calculs réalisés sur le corps K permettrait donc d'obtenir aussi un programme de calcul de l'inverse. Toutefois, mes tentatives d'implantations se sont révélées infructueuses. La trace complète, trop grande et comportant de nombreuses opérations inutiles, ne tarde pas à saturer la mémoire. Si l'on tente un nettoyage de la trace en cours de calcul, les temps deviennent prohibitifs. Je suis néanmoins convaincu que cette méthode devrait aboutir, avec une meilleure approche de son implantation.

B) La détermination des superpositions dans l'algorithme de base canonique, ainsi que des syzygies dans l'algorithme de base standard généralisé pose le problème de résoudre certaines équations diophantiennes. La méthode que j'ai utilisée pour les bases canoniques, par un calcul préalable de base standard paraît raisonnable en pratique et possède ses avantages. Il serait pourtant utile de la comparer avec d'autres méthodes, comme celles de HUET.

C) La détermination des syzygies pour les bases standard d'idéaux différentiels pose aussi un problème algorithmique, dont la solution proposée ici ne me satisfait guère par sa brutalité.

2. Problèmes de finitudes. Calcul des ensembles caractéristiques

On a rencontré des problèmes de finitude pour deux types de généralisation des bases standard : les bases caconiques et les bases standard d'idéaux différentiels. Dans le premier cas, on a donné une conjecture. Supposons qu'on puisse en donner une preuve effective, c'est-à-dire déterminer explicitement un élément de la clôture intégrale non présent dans l'algèbre, si la base canonique n'est pas de type fini. On a alors montré au chapitre III § 3, comment on pourrait tester l'appartenance à la sous-algèbre par le calcul de base canonique finie, et d'une base standard généralisée.

Dans le cas des idéaux différentiels, bien des efforts restent à faire sans doute pour définir un test d'appartenance. On a souligné au chap. IV § 1 quelques cas sympathiques où l'on peut conclure même si la base est infinie.

Enfin, le problème reste ouvert de déterminer l'ensemble caractéristique d'un idéal. Par chance, pour les applications du chapitre V, on pouvait déjà partir d'un ensemble caractéristique. Dans le cas général, une méthode reste à inventer.

3. Problèmes de complexité

On a pu donner des résultats de complexité pour tester l'existence de l'inverse d'une application rationnelle différentielle, et exprimer l'inverse d'une application rationnelle *algébrique* $f : \mathbf{A}^n \mapsto \mathbf{A}^n$. On souhaiterait pouvoir les étendre, sous une forme que j'ignore, à des applications rationelles plus générales, par exemple en bornant aussi le degré de l'inverse d'une application rationnelle différentielle, ou en considérant aussi des applications $f : X \subset \mathbf{A}^n \mapsto \mathbf{A}^m$.

Pour les applications à l'automatique, on souhaiterait avoir une estimation de la taille des résumés exhaustifs obtenus par la méthode du chap. V § 6, ce qui n'est pas évident.

Un problème de base serait d'obtenir un nullstellensatz effectif différentiel, sous la forme suivante. Si

$$1 = \sum_{i=1}^{r} R_i\, \theta_i\, P_{j_i} \in [P_j\ j = 1, \ldots, s]_{\mathcal{F}\{x_1, \ldots, x_n\}}$$

majorer l'ordre et le degré des $m_i \theta_i P_{j_i}$ en fonction de s, de l'ordre et du degré maximal des P_j. Une majoration sur l'ordre permettrait d'ailleurs une majoration brutale du degré en appliquant le nullstellensatz effectif algébrique, comme on l'a fait en IV.1.

4. Calcul de résumés exhaustifs

Comme on l'a évoqué à la fin du chapitre V, un certain nombre de problèmes restent en suspens. L'un d'eux est de savoir si le fait d'autoriser des commandes non génériques peut changer les conclusions, ce qui paraît intuitivement peut probable.

Il serait très fructueux de pouvoir déterminer si la solution définie par les conditions initiales est générique. On pourrait alors élargir le champ des applications, et surtout traiter des structures très générales si l'on savait aussi dans les mauvais cas déterminer un idéal plus petit, définissant une structure "minimale" correspondant au processus modélisé.

On a brièvement évoqué le test de discernabilité, qui revient en fait à tester l'inclusion de deux variété algébriques différentielles. Parmis d'autres, cette question montre que les besoins de l'automatique peuvent introduire ou motiver des problèmes théoriques difficiles et en eux-mêmes très interessants.

Appendices

APPENDICE A

Un exemple de session en Scratchpad II

On donne à titre d'exemple une session de démonstration qui illustre les possibilités offertes par l'implantation réalisée en Scratchpad II des méthodes décrites au chap. V § 5.

```
)r demo1
     reading file DEMO1 INPUT A1
     Scratchpad
  )lo conp idpack structls

     loading CONP LISPLIB A1 for package ConvPack
     library CONP has been loaded and is now exposed.
     loading IDPACK LISPLIB A1 for package IdentifiabilitePackage
     library IDPACK has been loaded and is now exposed.
     loading STRUCTLS LISPLIB A1 for domain StructureLineaireStationnaire
     library STRUCTLS has been loaded and is now exposed.
  )time on

   St:=STRUCTLS
     loading LIBNAME LISPLIB K2 for domain LibraryName
     loading FNAME LISPLIB K2 for domain FileName
     loading RF LISPLIB K2 for domain RationalFunction
     loading KAF LISPLIB K1 for domain KeyedAccessFile

     (1)  STRUCTLS

     Type: DOMAIN  .536 (IN) + 7.138 (OT) = 7.674 sec

   -- comment entrer une structure

   strSimp:=new(2,1,1,[th1,th2,th3])$St

     (2)
     dX  |0  0|     |0|
     --= |     |X + | |U
     dt  |0  0|     |0|
     Y = [0  0]X
     Parametres internes = [th1,th2,th3]
```

```
  Type: STRUCTLS  .283 (IN) + .234 (EV) + .297 (OT) = .814 sec

-- echange entre compartiments

etat(strSimp,1,2,th1)

  (3)
  dX  |- th1  0|    |0|
  --= |        |X + | |U
  dt  | th1   0|    |0|
  Y = [0  0]X
  Parametres internes = [th1,th2,th3]

  Type: STRUCTLS   .349 (IN) + .017 (EV) + .134 (OT) = .5 sec

etat(strSimp,2,1,th2)

  (4)
  dX  |- th1   th2 |    |0|
  --= |            |X + | |U
  dt  | th1   - th2|    |0|
  Y = [0  0]X
  Parametres internes = [th1,th2,th3]

  Type: STRUCTLS  .075 (IN) + .017 (EV) + .028 (OT) = .12 sec

-- sortie du systeme
etat(strSimp,2,th3-th2)

  (5)
  dX  |- th1   th2 |    |0|
  --= |            |X + | |U
  dt  | th1   - th3|    |0|
  Y = [0  0]X
  Parametres internes = [th1,th2,th3]

  Type: STRUCTLS  .203 (IN) + .036 (EV) + .1 (OT) = .339 sec
-- on commande le compartiment 1 com(strSimp,1,1,1)

  (6)
  dX  |- th1   th2 |    |1|
  --= |            |X + | |U
  dt  | th1   - th3|    |0|
  Y = [0  0]X
  Parametres internes = [th1,th2,th3]

  Type: STRUCTLS   .1 (IN) + .016 (EV) + .082 (OT) = .199 sec

-- on observe le compartiment 1
obs(strSimp,1,1,1)

  (7)
  dX  |- th1   th2 |    |1|
  --= |            |X + | |U
  dt  | th1   - th3|    |0|
  Y = [1  0]X
  Parametres internes = [th1,th2,th3]

  Type: STRUCTLS  .056 (IN) + .016 (EV) + .088 (OT) = .16 sec
```

```
-- voici la structure strSimp

  (8)
  dX  |- th1   th2 |    |1|
  --= |            |X + | |U
  dt  | th1   - th3|    |0|
  Y = [1  0]X
  Parametres internes = [th1,th2,th3]

  Type: STRUCTLS  .004 (IN) + .024 (OT) = .027 sec

-- calcul du resume exhaustif pour la matrice de transfert
resumExhTransfert strSimp

  (9)  [th3,1,1,th3 + th1,th1 th3 - th1 th2]

  Type: L P I  .021 (IN) + 1.737 (EV) + .239 (OT) = 1.996 sec

-- test d'identifiabilite
identifiable?(strSimp,"Transfert")
  loading NDMP LISPLIB K1 for domain
  NewDistributedMultivariatePolynomial
  loading NDP LISPLIB K1 for domain NewDirectProduct
  loading OV LISPLIB K1 for domain OrderedVarlist
  loading GB LISPLIB K1 for package GroebnerPackage
  loading GBINTERN LISPLIB K1 for package GroebnerInternalPackage

  (10)  true

  Type: B   .094 (IN) + 8.584 (EV) + 5.198 (OT) + 2.04 (GC) = 15.916 sec

-- observation d'un bestiaire
-- exemples tires de la these de Y. Lecourtier, stockes sur disque
liLec:=liste("Lecourt these a")$St

  (11)
  ["methane p. 13", "exemple simple p. 31", "chimiotherapie p. 41", "p. 45",

   "p. 47", "premier passage p. 106", "premier passage theta5 = 0",

   "discernabilite exemple M p. 124", "discernabilite exemple M' p. 124"]


  Type: L S .096 (IN) + .467 (EV) + .179 (OT) = .742 sec

-- Un exemple: effet de premier passage d'un medicament
-- Voir ex. V.5.1.1
pp1:=get("Lecourt these a",liLec.6)$St

  (12)
      |- th2 - th1    0      0  |    |1|
  dX  |                         |    | |
  --= |    th1      - th3    0  |X + |0|U
  dt  |                         |    | |
      |    th2       th3   - th4|    |0|

      |0  th6   0 |
  Y = |           |X
```

```
      |0   0   th7|

  Parametres internes = [th1,th2,th3,th4,th6,th7]

  Type: Union(STRUCTLS,"failed")
          .654 (IN) + .122 (EV) + .333 (OT) = 1.11 sec

resumExhTransfert pp1

  (13)
  [(th2 + th1)th3 th7, th2 th7, 1, th4 + th3 + th2 + th1,

   (th3 + th2 + th1)th4 + (th2 + th1)th3, (th2 + th1)th3 th4, th1 th6, 1,

   th3 + th2 + th1, (th2 + th1)th3]


  Type: L P I  .026 (IN) + .648 (EV) + .038 (OT) = .712 sec

identifiable?(pp1,"Transfert")

  (14)  false

  Type: B.06 (IN) + 3.584 (EV) + .027 (OT) = 3.671 sec

-- Regardons la base standard
par:=lParms(pp1)$St

  (15)  [th1,th2,th3,th4,th6,th7]

  Type: L E .095 (IN) + .015 (EV) + .116 (OT) = .226 sec
ndmp:=NDMP(par,RF(I))

  (16)  NDMP([th1,th2,th3,th4,th6,th7],RF I)

  Type: DOMAIN         .088 (IN) + .062 (OT) = .15 sec

std:=zap(stdT(pp1))$ZAP(L E, L ndmp)
  loading ZAP LISPLIB K2 for package ZweitypeAlterationPackage

  (17)
                      2
      2   (- Th3 + Th2 - Th1)Th6       Th1 Th6
  [th6  + ---------------------- th6 + ---------,
                Th3 - Th2              Th3 - Th2

        Th3 - Th2
   th1 + --------- th6 - Th3 + Th2 - Th1, th2 - Th2,
           Th6

        - Th3 + Th2
   th3 + ----------- th6 - Th2, th4 - Th4, th7 - Th7]
            Th6


  Type: L NDMP([th1,th2,th3,th4,th6,th7],RF I)
          .172 (IN) + .037 (EV) + .597 (OT) = .805 sec
std.0
```

```
   2
            2   (- Th3 + Th2 - Th1)Th6       Th1 Th6
  (18)  th6  + --------------------- th6 + --------
                     Th3 - Th2               Th3 - Th2

  Type: NDMP([th1,th2,th3,th4,th6,th7],RF I)
           .46 (IN) + .018 (EV) + .101 (OT) = .579 sec


-- d'apres la forme de la base standard, il y a deux solutions.
-- un exemple de discernabilite
dis1:St:=get("Lecourt these a","p. 45")$St

  (19)
  dX  |    - th1      th2 |    |1|
  --= |                   |X + | |U
  dt  |- th3 + th1  - th2|    |0|
  Y = [1  0]X
  Parametres internes = [th1,th2,th3]

  Type: STRUCTLS .097 (IN) + .104 (EV) + .044 (OT) = .246 sec
dis2:St:=get("Lecourt these a","p. 47")$St

  (20)
  dX  |    - th1     th2|    |1|
  --= |                 |X + | |U
  dt  |- th3 + th1  - 1|    |0|
  Y = [1  0]X
  Parametres internes = [th1,th2,th3]

  Type: STRUCTLS .078 (IN) + .103 (EV) + .041 (OT) = .223 sec

Un exemple de discernabilite (voir V.5.2)
distingable?(dis1,dis2,"Transfert")

  (21)  true

  Type: Union(B,"failed") .077 (IN) + .32 (EV) + .092 (OT) = .488 sec

distingable?(dis2,dis1,"Transfert")

  (22)  false

  Type: Union(B,"failed") .064 (IN) + .09 (EV) + .021 (OT) = .175 sec
  0  total errors
```

Le fichier suivant correspond au traitement complet de l'exemple V.5.1.2.

```
)r demo2
  reading file DEMO2 INPUT A1
  Scratchpad

)time on
St:=STRUCTLS

  (23)  STRUCTLS

  Type: DOMAIN .096 (IN) + .262 (OT) = .358 sec
liRak:=liste("Raksanyi these a")$St
```

```
  (24)
  ["Synthese de l'ammoniacp. 117", "premier passage p. 121",

   "synthese de l'amoniac p. 117", "ammoniac", "ammoniac p. 115"]


  Type: L S .138 (IN) + .489 (EV) + .433 (OT) = 1.06 sec
Ammon:St:=get("Raksanyi these a",liRak.0)$St

  (25)
  dX
  --= matrix1 X + matrix2 U
  dt
  Y = matrix3 X
  Parametres internes = [f2,v13,v21,v31,v32]


where matrix1 =
  [[- f1 v31 - f1 v21 - f1 v01,f1 v12,f1 v13,0,0],

   [f2 v21,- f2 v32 - f2 v12,f2 v23,0,0],

   [f3 v31,f3 v32,- f3 v43 - f3 v23 - f3 v13,f3 v34,0],

   [0,0,f4 v43,- f4 v54 - f4 v34,f4 v45],

   [0,0,0,f5 v54,- f5 v45 - f5 v05]]


and matrix2 =
  |0|
  | |
  |0|
  | |
  |0|
  | |
  |0|
  | |
  |1|

and matrix3 =
  |0  0  0  0  1|
  |             |
  |1  0  0  0  0|

  Type: STRUCTLS .738 (IN) + .161 (EV) + .279 (OT) = 1.178 sec
matA:=a Ammon;

  Type: VOID .046 (IN) + .015 (EV) + .023 (OT) = .084 sec

-- On tient compte du fait que le systeme est stationnaire,
-- et qu'il y a donc des relations lineaires entre les parametres :
--   v45 = v01+-v54, v34 = v43+v01, v23 = v32+v01+v31-v13,
--   v12 = v01+v21+v31-v13, v = v01+v05.

for i in 0..2 repeat
  for j in 0..2 repeat
     matA.i.j:= eval(matA.i.j,[v45,v34,v23,v12,v],
                              [v01+v54,v43+v01,v32+v01+
```

```
                          v31-v13,v01+v21+v31-v13,v01+v05])

  Type: VOID 3.319 (IN) + 2.967 (EV) + .886 (OT) = 7.172 sec

-- Compte tenu de la forme particuliere de la structure,
-- un resume exhaustif s'obtient en considerant les coefficients
-- des polynomes caracteristiques des sous matrices principales
-- d'ordre 2 et 3

matA3Rf:M RF I:= new(3,3,0$RF(I));

  Type: VOID .276 (IN) + .027 (EV) + .282 (OT) = .585 sec for i in 0..2 repeat
 for j in 0..2 repeat
     matA3Rf.i.j:= matA.i.j

  Type: VOID
  14.928 (IN) + 1.664 (EV) + 1.036 (OT) + 2.22 (GC) = 19.848 sec

carF:= characteristicpol matA3Rf;
  loading EP LISPLIB K1 for package EigenPackage
  loading SOLVERAD LISPLIB K1 for package RadicalSolvePackage
  loading Q2ZPOLY LISPLIB K2 for package RationalToIntegerPolynomial
  loading RE LISPLIB K2 for domain RadicalExtension
  loading SR LISPLIB K2 for domain SortedRadicals
  loading DEGRED LISPLIB K2 for package DegreeReductionPackage
  loading SOLVEFOR LISPLIB K1 for package PolynomialSolveByFormulas
  loading EQ LISPLIB K2 for domain Equation
  loading SY LISPLIB K1 for domain Symbol
  loading SUCH LISPLIB K2 for domain SuchThat


  Type: VOID .189 (IN) + 4.728 (EV) + 17.681 (OT) + 4.55 (GC) = 27.147 sec

  -- Quelle horreur, pour calculer un polynome caracteristique...

carP:P I:=numer carF;

  Type: VOID .204 (IN) + .016 (EV) + .053 (OT) = .274 sec
carSUP:= likeUniv(carP,%A);

  Type: VOID .142 (IN) + .148 (EV) + .047 (OT) = .337 sec
resum3:=listCoef carSUP

  (33)

...

  Type: L P I .046 (IN) + .016 (EV) + .162 (OT) = .224 sec
matA2Rf:M RF I:= new(2,2,0$RF(I));

  Type: VOID .221 (IN) + .28 (EV) + .083 (OT) = .584 sec

for i in 0..1 repeat
 for j in 0..1 repeat
     matA2Rf.i.j:= matA.i.j

  Type: VOID 1.455 (IN) + .866 (EV) + .119 (OT) = 2.439 sec

carF:= characteristicpol matA2Rf;
```

```
  Type: VOID .055 (IN) + .785 (EV) + .018 (OT) = .857 sec

carP:P I:=numer carF;

  Type: VOID .087 (IN) + .017 (EV) + .024 (OT) = .128 sec
carSUP:= likeUniv(carP,%B);

  Type: VOID .118 (IN) + .05 (EV) + .015 (OT) = .183 sec
resum2:=listCoef carSUP

  (39)

...


  Type: L P I .039 (IN) + .018 (EV) + .045 (OT) = .102 sec

resum:= append(resum2,resum3)

  (40)

...


  Type: L P I .107 (IN) + .019 (EV) + .109 (OT) = .235 sec
resumExhSpecial(Ammon,resum);

  Type: VOID .038 (IN) + .017 (EV) + .071 (OT) = .126 sec
changeLE(Ammon,[v13,v21,v31,v32,f2])$St;

  Type: VOID .307 (IN) + .309 (EV) + .088 (OT) = .704 sec

identifiable?(Ammon,"Special")$St

  (43)  false

  Type: B .093 (IN) + 46.711 (EV) + 1.279 (OT) + 10.182 (GC) = 58.265 sec

par:=lParms(Ammon)$St;

  Type: VOID .303 (IN) + .303 (EV) + .092 (OT) = .698 sec
ndmp:=NDMP(par,RF(I))

  (45)  NDMP([v13,v21,v31,v32,f2],RF I)

  Type: DOMAIN .092 (IN) + .118 (OT) = .21 sec

std:=zap(stdS(Ammon))$ZAP(L E, L ndmp)

  (46)

...


  Type: L NDMP([v13,v21,v31,v32,f2],RF I)
          .184 (IN) + .036 (EV) + .399 (OT) = .619 sec

lIn:=[degree pol for pol in std]
```

```
(47)
[[1,1,0,0,0], [0,2,0,0,0], [1,0,0,1,0], [1,0,0,0,1], [0,1,0,0,1],

 [0,0,0,1,1], [0,0,1,0,0]]

Type: L NDP(5,NNI) .088 (IN) + .704 (EV) + .375 (OT) = 1.166 sec
```

On récupère ainsi la liste des multidegrés des monômes de tête, et l'on en conclut qu'il y a une infinité de solutions, car l'idéal est de dimension 1.

APPENDICE B

Code source

On trouvera ici le code source des packages ou domaines évoqués dans le texte. On se reportera à [Scr] pour la syntaxe de Scratchpad II.

§ 1. IDENTIFIABILITÉ

1. CONVPACK

Ce package réalise quelques coercions utiles pour IDPACK : la fonction *mkeqQ* prend une fraction $f_i = P_i/Q_i$ et retourne $Q_i(y)P_i(x) - P_i(y)Q_i(x) \in \mathbf{Q}(y)[x]$. Une variante *mkeqP* traite le cas où f_i est un polynôme. La fonction *mkeqDiv* retourne $Q_i(x)u_i - 1$.

```
)abb package CONP ConvPack

ConvPack(le:List Expression):Public == Prive where
   E ==> Expression
   SE ==> SortedExpressions
   L ==> List
   LE ==> L E
   I ==> Integer
   PI  ==> Polynomial I
   RFI ==> RationalFunction I
   NDMP ==> NewDistributedMultivariatePolynomial(le,RFI)
   OV ==> OrderedVarlist le
   Public == with
     convertP : PI            -> NDMP
     mkeqP    : (PI,PI)       -> NDMP
     mkeqQ    : (RFI,RFI)     -> NDMP
     mkeqP    : PI            -> NDMP
     mkeqQ    : RFI           -> NDMP
     mkeqP    : PI            -> NDMP
     mkeqQ    : RFI           -> NDMP
     mkeqDiv  : (PI,E)        -> NDMP
   Prive == add
```

```
-- fonctions locales
   ov        : E   - > OV
   convertP1:(PI,L E) - > NDMP

-- implantation
   mkeqDiv(pol,e) ==
      convertP(pol) * varPol(ov(e))$NDMP - 1
   ov(ex) == (coerce(ex)$OV):OV
   convertP1(pol,l) ==
      null(l) => pol::RFI::NDMP
      ex:=l.0
      se:=ex::SE
      ¬ member(se,varlist pol) => convertP1(pol,rest l)
      var:=varPol(ov ex)$NDMP
      upol:=likeUniv(pol,se)
      res:NDMP:=0
      while upol ¬ = 0 repeat
         res:= res + var**(degree upol)*convertP1(lc upol,rest l)
         upol:=red upol
      res

   convertP(pol:PI) ==
      l:=le
      convertP1(pol,l)

   mkeqP(pol1:PI,pol2:PI) ==
      convertP(pol2)-pol1::RFI::NDMP

   mkeqQ(rat1:RFI,rat2:RFI) ==
      pol1:PI:=numer(rat2)
      pol2:PI:=denom(rat2)
      convertP(pol1)-convertP(pol2)*rat1::NDMP

   mkeqP(pol:PI) ==
      convertP(pol)-pol::RFI::NDMP

   mkeqQ(rat:RFI) ==
      pol1:PI:=numer(rat)
      pol2:PI:=denom(rat)
      convertP(pol1)-convertP(pol2)*rat::NDMP
```

2. IDPACK

Ce package teste l'identifiabilité par la méthode de l'idéal Δ. Il traite aussi la discernabilité en vérifiant qu l'idéal obtenu est trivial (voir chap. V § 5 n° 2). La fonction *identifiable* prend comme premier argument un résumé exhaustif, comme second la liste des paramètres a priori inconnus et comme troisième argument la liste des paramètres dont on veut tester l'identifiabilité. Par défaut, s'il n'y a pas de troisième argument, on teste l'identifiabilité de tous les paramètres.

```
)abb package IDPACK IdentifiabilitePackage

IdentifiabilitePackage(): Public == Prive where
    L      ==> List
    E      ==> Expression
```

```
SE     ==> SortedExpressions
I      ==> Integer
NNI    ==> NonNegativeInteger
PI     ==> Polynomial I
RFI    ==> RationalFunction I
NDMP   ==> NewDistributedMultivariatePolynomial
NDP    ==> NewDirectProduct
GB     ==> GroebnerPackage
CONP   ==> ConvPack
Public == with
  distingable?  : (L PI,L PI,L E)        -> Boolean
  distingable?  : (L RFI,L RFI,L E)      -> Boolean
  identifiable? : (L PI,L E)             -> Boolean
  identifiable? : (L RFI,L E)            -> Boolean
  identifiable? : (L PI,L E,L E)         -> Boolean
  identifiable? : (L RFI,L E,L E)        -> Boolean
  lpP           : ()                     -> L PI
  putlpP        : L PI                   -> L PI
  stdP          : ()                     -> L E
  leP           : ()                     -> L E
  putleP        : L E                    -> L E
  putstdP       : L E                    -> L E
  lpQ           : ()                     -> L RFI
  putlpQ        : L RFI                  -> L RFI
  stdQ          : ()                     -> L E
  leQ           : ()                     -> L E
  putleQ        : L E                    -> L E
  putstdQ       : L E                    -> L E
Prive == add
-- On garde en memoire les arguments du dernier calcul de base standard
-- pour eviter de la recalculer inutilement
  memo:Record(LPP:L PI,LPQ:L RFI,LEP:L E,LEQ:L E,STDP:L E,_
              STDQ:L E) := [[],[],[],[],[],[]]

-- fonctions locales

-- implantation

-- cas particulier ou le resume est polynomial
  distingable?(lp1:L PI,lp2:L PI,le2:L E):Boolean ==
    ndmp:= NDMP(le2,RFI)
    lndmp:= L ndmp
    conp:=CONP(le2)
    ndp:=NDP(£ le2,NNI)
    systeme:L ndmp:=
      [mkeqP(pol1,pol2)$conp for pol1 in lp1 for pol2 in lp2]
    systeme:=removeDuplicates systeme
    systeme:=delete(0$ndmp,systeme)$L(ndmp)
    gb:=GB(RFI,ndp,ndmp)
    resu:=groebner(systeme)$gb
    resu.0 =1$ndmp => true
    false

-- cas general rationnel
  distingable?(lp1:L RFI,lp2:L RFI,le2:L E):Boolean ==
    lden:L PI:=[]
    for rat in lp2 repeat
      if ¬ isconst?(pol:=denom(rat)) then lden:=cons(pol,lden)
    lden:=removeDuplicates lden
```

```
    lvDiv:L E:=[i::E for i in 1..(£ lden)]
    leSys:=append(le2,lvDiv)
    ndmp:=NDMP(leSys,RFI)
    lndmp:=L ndmp
    ndp:=NDP(£ leSys,NNI)
    conp:=CONP(leSys)
    -- on fabrique le systeme engendrant l'ideal J (chap. V.5.2 p. 112)
    systeme:L ndmp:=
      [mkeqQ(pol1,pol2)$conp for pol1 in lp1 for pol2 in lp2]
    systeme:=removeDuplicates systeme
    systeme:=delete(0$ndmp,systeme)$L(ndmp)
    sysDiv:L ndmp:=
      [mkeqDiv(pol,e) for pol in lden for e in lvDiv]
    systeme:=append(systeme,sysDiv)
    gb:=GB(RFI,ndp,ndmp)
    resu:=groebner(systeme)$gb
    --  on teste que l'ideal est trivial
    resu.0 =1$ndmp => true
    false

--  cas polynomial
  identifiable?(lp:L PI,le:L E,lVar:L E):Boolean ==
    ndmp:=NDMP(le,RFI)
    lndmp:= L ndmp
    conp:=CONP(le)
    sol:lndmp:= if lp=lpP() and le=leP() then stdP():lndmp else
      ndp:=NDP(£ le,NNI)
      systeme:L ndmp:=[mkeqP(pol)$conp for pol in lp]
      systeme:=removeDuplicates systeme
      systeme:=delete(0$ndmp,systeme)$L(ndmp)
      gb:=GB(RFI,ndp,ndmp)
      resu:=groebner(systeme)$gb
      putlpP(lp)
      putstdP(resu:L(E))
      putleP(le)
      resu:lndmp
    etalon:L ndmp:=[mkeqP(varPol(e::SE)$PI)$conp for e in lVar]
    for np in etalon repeat
      ¬ member(np,sol) => return false
    true

--  cas rationnel
  identifiable?(lp:L PI,le:L E):Boolean  ==
    identifiable?(lp,le,le)

  identifiable?(lp:L RFI,le:L E,lVar:L E):Boolean ==
    lden:L PI:=[]
    for rat in lp repeat
      if ¬ isconst?(pol:=denom(rat)) then lden:=cons(pol,lden)
    lden:=removeDuplicates lden
    lvDiv:L E:=[i::E for i in 1..(£ lden)]
    leSys:=append(le,lvDiv)
    ndmp:=NDMP(leSys,RFI)
    lndmp:=L ndmp
    conp:=CONP(leSys)
    sol:lndmp:= if lp=lpQ() and le=leQ() then stdQ():lndmp else
      ndp:=NDP(£ leSys,NNI)
      --  on fabrique le systeme engendrant l'ideal J du th. III.2.3.3 p.51
      systeme:L ndmp:=[mkeqQ(rat)$conp for rat in lp]
```

```
      systeme:=removeDuplicates systeme
      systeme:=delete(0$ndmp,systeme)$L(ndmp)
      sysDiv:L ndmp:=
        [mkeqDiv(pol,e) for pol in lden for e in lvDiv]
      systeme:=append(systeme,sysDiv)
      gb:=GB(RFI,ndp,ndmp)
      resu:=groebner(systeme)$gb
      putlpQ(lp)
      putstdQ(resu:L(E))
      putleQ(le)
      resu:lndmp
    etalon:L ndmp:=[mkeqP(varPol(e::SE)$PI)$conp for e in lVar]
    for np in etalon repeat
      -- on teste que xi - yi est dans l'ideal
      ¬ member(np,sol) => return false
    true

  identifiable?(lp:L RFI,le:L E):Boolean ==
    identifiable?(lp,le,le)

  stdP() == memo.STDP
  putstdP(le) == memo.STDP := le
  stdQ() == memo.STDQ
  putstdQ(le) == memo.STDQ := le
  lpP() == memo.LPP
  lpQ() == memo.LPQ
  putlpP(lp) == memo.LPP:=lp
  putlpQ(lr) == memo.LPQ:=lr
  leP()==memo.LEP
  leQ()==memo.LEQ
  putleP(le)==memo.LEP:=le
  putleQ(le)==memo.LEQ:=le
```

3. STRUCTLS

Ce domaine modélise les structures linéaines stationnaires avec conditions initiales nulles.

```
-- Address comments and questions to
--   François OLLIVIER
--   Laboratoire d'Informatique de L'X (LIX)
--   Ecole Polytechnique
--   91 128 Palaiseau cedex (FRANCE)
--   BITNET: CFFOLL@FRPOLY11

)abb domain STRUCTLS StructureLineaireStationnaire

StructureLineaireStationnaire():Public == Prive where
  I     ==> Integer
  PI    ==> PositiveInteger
  L     ==> List
  E     ==> Expression
  S     ==> String
  Pol   ==> Polynomial I
  M     ==> Matrix Pol
  SUPol ==> SparseUnivariatePolynomial Pol
```

```
Pol2  ==> QuotientField SUPol
M2    ==> Matrix Pol2
ID    ==> IdentifiabilitePackage

Public == Set with
   new                 :  (I,I,I,L E)       -> $
   changeA             :  ($,I,I,Pol)       -> $
   changeB             :  ($,I,I,Pol)       -> $
   changeC             :  ($,I,I,Pol)       -> $
   changeLE            :  ($,L E)           -> $
   etat                :  ($,I,I,Pol)       -> $
   etat                :  ($,I,Pol)         -> $
   com                 :  ($,I,I,Pol)       -> $
   obs                 :  ($,I,I,Pol)       -> $
   matriceDeTransfert  :  $                 -> M2
   resumExhMarkov      :  $                 -> L Pol
   resumExhTransfert   :  $                 -> L Pol
   resumExhSpecial     :  $                 -> L Pol
   resumExhSpecial     :  ($,L Pol)         -> L Pol
   detXidMoinsA        :  $                 -> L Pol
   minDetXidMoinsA     :  ($,I,I)           -> L Pol
   get                 :  (S,S)             -> Union($,"failed")
   save                :  ($,S,S)           -> $
   liste               :  S                 -> L S
   distingable?        :  ($,$,S)           -> Union(Boolean,"failed")
   identifiable?       :  ($,S)             -> Boolean
   identifiable?       :  ($,L E,S)         -> Boolean
   a                   :  $                 -> M
   b                   :  $                 -> M
   c                   :  $                 -> M
   stdM                :  $                 -> L E
   stdT                :  $                 -> L E
   stdS                :  $                 -> L E
   lParms              :  $                 -> L E

 Prive == add
-- La representation interne contient le trois matrices,
-- la liste des coefficients inconnus, les resumes deja
-- calcules, ainsi que les bases standard correspondant
-- aux tests d'identifiabilite, pour eviter de repeter
-- les calculs. coefficient
   Rep:=Record(A:M,B:M,C:M,LE:L E,REM:L Pol,RET:L Pol,RES:L Pol,_
               STDM:L E,STDT:L E,STDS:L E)

   KAF:= KeyedAccessFile $
   LIB:= LibraryName
   lvP:L Pol:=[]
   lvE:L E:=[]



 --  fonctions locales
   liscoe    : SUPo   -> L Pol
   move      : Pol    -> Pol2
   move2     : M      -> M2
   createKaf : S      -> KAF
-- pour oublier les calculs deja faits sur une structure
   reset     : $      -> $
```

```
-- implantation

   liscoe(supol:SUPol):L Pol ==
      resu:L Pol:=[0$Pol for i in 0..(degree supol)]
      while supol ¬ = 0 repeat
         resu.(degree supol):=lc supol
         supol:=reductum supol
      resu

   move(pol:Pol):Pol2 == pol::SUPol::Pol2

   move2(mat:M):M2 ==
      nr:=nrows(mat)
      nc:=ncols(mat)
      ir:=nr::I -1
      ic:=nc::I -1
      mat2:=zero(nr,nc)$M2
      for i in 0..ir repeat
         for j in 0..ic repeat
            mat2.i.j:=move(mat.i.j)
      mat2

   reset(struct:$):$ ==
      struct.REM:=lvP
      struct.RET:=lvP
      struct.RES:=lvP
      struct.STDM:=lvE
      struct.STDT:=lvE
      struct.STDS:=lvE
      struct

   createKaf(fich:S):KAF ==
      libf:=find(fich)$LIB
      lib:LIB:=
         libf case "failed" => new(fich)$LIB
         libf::LIB
      open(lib)$KAF

-- fonction de sortie
   coerce(s:$):E ==
      eA:=(s.A)::E
      eB:=(s.B)::E
      eC:=(s.C)::E
      ligne1:=mkBinary(_=::E,mkBinary(_/::E,dX::E,dt::E),
      mkBinary(_+::E,mkBinary(_*::E,eA,X::E),mkBinary(_*::E,eB,U::E)))
      ligne2:=mkBinary(_=::E,"Y "::E,mkBinary(_*::E,eC,X::E))
      ligne3:=mkBinary(_=::E,"Parametres internes "::E,(s.LE)::E)
      mkBinary(SC::E,ligne1,mkBinary(SC::E,ligne2,ligne3))

-- fonction d'ecriture sur disque
   save(s:$,fich:S,nom:S):$ ==
      kaf:=createKaf(fich)
      setelt(kaf,nom,s)$KAF

-- fonction de lecture sur disque
   get(fich:S,nom:S):Union($,"failed") ==
      kaf:=createKaf(fich)
      search(kaf,nom)$KAF
```

```
    liste(fich:S):L S == keys createKaf fich

 -- fonctions d'entree

    new(r,p,q,le) ==
       [zero(r,r)$M,zero(r,p)$M,zero(q,r)$M,le,_
        lvP,lvP,lvP,lvE,lvE,lvE]$Rep

-- passage du compartiment i au compartiement j avec la constante pol
    etat(struct,i,j,pol) ==
       i:=i-1
       j:=j-1
       A1:=struct.A
       A1.i.i:=A1.i.i - pol
       A1.j.i:=A1.j.i + pol
       reset struct
-- evacuation du compartiment i avec la constante pol
    etat(struct,i,pol) ==
       i:=i-1
       A1:=struct.A
       A1.i.i:=A1.i.i - pol
       reset struct
-- commande du compartiment i par uj avec la constante pol
    com(struct,i,j,pol) ==
       i:=i-1
       j:=j-1
       B1:=struct.B
       B1.i.j:= pol
       reset struct
   -- la mesure du compartiment j avec la constante pol est yi
    obs(struct,i,j,pol) ==
       i:=i-1
       j:=j-1
       C1:=struct.C
       C1.i.j:=pol
       reset struct

-- pour changer une des trois matrices A, B ou C
-- (voir def. V.1.3.2 p. 105)
    changeA(s,i,j,pol) ==
       i:=i-1
       j:=j-1
       s.A.i.j:=pol
       reset s
    changeB(s,i,j,pol) ==
       i:=i-1
       j:=j-1
       s.B.i.j:=pol
       reset s
    changeC(s,i,j,pol) ==
       i:=i-1
       j:=j-1
       s.C.i.j:=pol
       reset s

-- pour changer la liste des paramètres inconnus
    changeLE(s:$,le:L E):$ ==
       s.STDM:=lvE
       s.STDT:=lvE
```

```
    s.STDS:=lvE
    s.LE:=le
    s

-- fonctions de recuperation des valeurs de la representation interne
  a(s) == s.A
  b(s) == s.B
  c(s) == s.C
  lParms(s) == s.LE
  stdM(s) == s.STDM
  stdT(s) == s.STDT
  stdS(s) == s.STDS

-- Resumes exhaustifs
  resumExhMarkov(s) ==
    ¬ null(re:=s.REM) => re
    A2:=s.A
    B2:=s.B
    C2:=s.C
    r:=nrows(A2)
    SM:=SquareMatrix(r:PI,Pol)
    A3:=A2:SM
    lp:L Pol:=[]
    for i in 1..(2*r−1) repeat
      mat:M:=((C2 * (A3**i):M)::M * B2)::M
      lp:=append(ravel mat,lp)
    s.REM:=lp

  matriceDeTransfert(s) ==
    r:=nrows(s.A)
    SM:= SquareMatrix(r::PI,Pol2)
    A2:=move2(s.A):SM
    B2:=move2(s.B)
    C2:=move2(s.C)
    XX:=varPol()$SUPol::Pol2
    MX:=XX::SM
    A2:=MX−A2
    A3:=recip(A2):M2
    ((C2*A3)::M2 * B2)::M2


  resumExhTransfert(s) ==
    ¬ null(re:=s.RET) => re
    A2:=matriceDeTransfert(s)
    ir:=nrows(A2)::I − 1
    ic:=ncols(A2)::I − 1
    lp:L Pol:=[]
    for i in 0..ir repeat
      for j in 0..ic repeat
        frac:Pol2:=A2.i.j
        pd:SUPol:=denom frac
        lp:=append(listCoef pd,lp)
        pn:SUPol:=numer frac
        lp:=append(liscoe pn,lp)
    s.RET:=lp

  detXidMoinsA(s:$):L Pol ==
    A1:=s.A
    nr:=nrows A1
```

```
    SM:=SquareMatrix(nr:PI,Pol2)
    A2:=move2(A1):SM
    XX:=varPol()$SUPol::Pol2
    MX:=XX::SM
    A2:=MX−A2
    det:Pol2:=determinant A2
    listCoef(numer det)

  minDetXidMoinsA(s:$,i:I,j:I): L Pol ==
    i:=i−1
    j:=j−1
    A1:=s.A
    nr:=(nrows A1)−1
    ir:=nr−1
    SM:=SquareMatrix(nr:PI,Pol2)
    A2:=move2(A1)
    A3:=0$SM
    for ii in 0..ir repeat
      for jj in 0..ir repeat
        iii:=if ii < i then ii else ii+1
        jjj:=if jj < j then jj else jj+1
        A3.ii.jj:= A2.iii.jjj
    XX:=varPol()$SUPol::Pol2
    MX:=XX::SM
    A3:=MX−A3
    det:Pol2:=determinant A3
    listCoef(numer det)


-- pour donner explicitement un resume calcule par une autre methode
  resumExhSpecial(s:$,lp:L Pol):L Pol ==
    s.RES:=lp
  resumExhSpecial(s) == s.RES

 -- identifiabilite (utilise IDPACK)
  inpu ==> READSPADEXPR$Lisp

  distingable?(s1:$,s2:$,str:S):Union(Boolean,"failed") ==
    nrows a s1 ¬ = nrows a s2 => "failed"
    nrows b s1 ¬ = nrows b s2 => "failed"
    ncols c s1 ¬ = ncols c s2 => "failed"
    while(str¬ ="Markov" and str¬ ="Transfert") repeat
      SAY("Les options sont Markov et Transfert.")$Lisp
      SAY("Entrez votre option.")$Lisp
      str:=inpu()
    if str="Markov" then
      resu1:L Pol:=resumExhMarkov s1
      resu2:L Pol:=resumExhMarkov s2
    if str="Transfert" then
      resu1:L Pol:=resumExhTransfert s1
      resu2:L Pol:=resumExhTransfert s2
   -- appelle IDPACK
    distingable?(resu1,resu2,lParms s2)$ID

  identifiable?(s:$,lVar:L E,str:S) ==
    while(str¬ ="Markov" and str¬ ="Transfert" and str¬ ="Special")_
      repeat
        SAY("Les options sont Markov, Transfert et Special.")$Lisp
        SAY("Entrez votre option.")$Lisp
```

```
        str:=inpu()
    le:=lParms s
    lp:L Pol:=lvP
    boo1:Boolean:=true
    if str="Markov" then
        lp:=resumExhMarkov s
        std:=stdM s
        ¬ null std =>
          boo1:=false
          putleP(le)$ID
          putlpP(lp)$ID
          putstdP(std)$ID
      else if str="Transfert" then
          lp:=resumExhTransfert s
          std:=stdT s
          ¬ null std =>
            boo1:=false
            putleP(le)$ID
            putlpP(lp)$ID
            putstdP(std)$ID
        else
          lp:=resumExhSpecial s
          std:=stdS s
          ¬ null std =>
            boo1:=false
            putleP(le)$ID
            putlpP(lp)$ID
            putstdP(std)$ID
   -- appelle IDPACK
    boo:Boolean:=identifiable?(lp,le,lVar)$ID
    std:=stdP()$ID
   -- stocke la base standard, si ce n'est deja fait
    if boo1 then
      if str="Markov" then s.STDM:=std  else
        if str="Transfert" then s.STDT:=std else s.STDS:=std
    boo

  identifiable?(s,str) == identifiable?(s,lParms s,str)$$
```

§ 2. BASES CANONIQUES

1. MOFAM

Ce domaine implante le produit du monoïde des monômes en x et du monoïde libre engendré par l'ensemble des monoômes de tête, avec un ordre correspondant aux hypothèses de la prop. III.3.2.2.5 p. 57.

```
-- % MutableOrderedFreeAbelianMonoid
)abbrev domain MOFAM MutableOrderedFreeAbelianMonoid

MutableOrderedFreeAbelianMonoid(Mon): Exportation == Production where
```

```
Mon  : OrderedAbelianMonoidSup
I    ==> Integer
NNI  ==> NonNegativeInteger
E    ==> Expression
L    ==> List
SEX  ==> SExpression
OUT  ==> OutputPackage
Term ==> Record(gen: I, exp: NNI)
Tag  ==> List Term

Exportation ==> OrderedAbelianMonoidSup with
   coet      : I       -> $
   member?   : ($, I)  -> Boolean
   coev      : Mon     -> $
   new       : (I,Mon) -> $
   delete    : I       -> Void
   clearAll  : ()      -> Void
   lisTag    : ()      -> L I
   purTag?   : $       -> Boolean
   getTag    : $       -> L Record(gen: I, exp: NNI)
   eval      : $       -> Mon
   eval1     : Tag     -> Mon

Production ==> add
-- representation
-- Une partie "en x" val et une autre correspondant au monoide libre tag
   Rep:= Record(val: Mon,tag: Tag)

-- variable globale
   Rec:= Record(index:I,deg:Mon)
   LRec:= L Rec
-- On garde la liste des monomes de tete, car ils servent a definir l'ordre
   lTag:LRec:=[[0,0]]

   i: I
   f, g: $
   n: NNI
   m: I
   mon:Mon

 -- local
   getVal(m:I):Mon ==
      for cc in lTag.rest repeat
         cc.index = m => return cc.deg
      0$Mon

   sub(t:Term):E ==
      t.exp = 1 => mkBinary("SUB"::E,"p"::E,(t.gen)::E)
      mkBinary("*"::E,(t.exp)::E, mkBinary("SUB"::E,"p"::E,(t.gen)::E))

   plus(t1:Tag, t2:Tag):Tag ==
      t1 = [] => t2
      t2 = [] => t1
      term1:=t1.first
      term2:=t2.first
      term1.gen > term2.gen =>
         cons(term1,plus(t1.rest,t2))
      term1.gen < term2.gen =>
         cons(term2,plus(t2.rest,t1))
```

```
    cons([term1.gen,term1.exp + term2.exp],plus(t1.rest,t2.rest))

  moins(t1:Tag, t2:Tag):Union(Tag,"failed") ==
    t2 = [] => t1
    t1 = [] => "failed"
    term1:=t1.first
    term2:=t2.first
    term1.gen > term2.gen =>
      (bb:= moins(t1.rest,t2)) case "failed" => return "failed"
      cons(term1,bb::Tag)
    term1.gen < term2.gen => "failed"
    (aa:= term1.exp - term2.exp) case "failed" => return "failed"
    (bb := moins(t1.rest,t2.rest)) case "failed" => return "failed"
    cc:= bb::Tag
    aa = 0 => cc
    cons([term1.gen,aa::NNI],cc)

  sup1(t1:Tag, t2:Tag):Tag ==
    t1 = [] => t2
    t2 = [] => t1
    term1:=t1.first
    term2:=t2.first
    term1.gen > term2.gen =>
      cons(term1,sup1(t1.rest,t2))
    term1.gen < term2.gen =>
      cons(term2,sup1(t2.rest,t1))
    cons([term1.gen,sup(term1.exp,term2.exp)],sup1(t1.rest,t2.rest))

  mult(n:NNI, t1:Tag):Tag ==
    n = 0 => []
    [[term.gen,n * term.exp] for term in t1]

-- Ordre lexicographique inverse
  less(t1:Tag,t2:Tag):Boolean ==
    t1 = [] => false
    t2 = [] => true
    term1:=t1.first
    term2:=t2.first
    ind1:=term1.gen
    ind2:=term2.gen
    ind1 > ind2 => true
    ind1 < ind2 => false
    (exp1:=term1.exp) > (exp2:=term2.exp) => true
    exp1 < exp2 => false
    less(t1.rest,t2.rest)

-- fonctions exportees
  coet(m:I):$ == [0$Mon,[[m,1$NNI]]$Tag]$Rep

  member?(f,m) ==
    ft:=f.tag
    while ft ¬ = [] repeat
      (m2:=ft.first.gen) < m => return false
      m2 = m => return true
      ft:=ft.rest
    false


  coev(mon) == [mon,[]]
```

```
   getTag(f) == ((f:Rep).tag):L Record(gen:I,exp:NNI)

   new(m:I,mon:Mon):$ ==
     lTag.rest:=cons([m,mon]$Rec,lTag.rest)
     coet(m)

   delete(m:I):Void ==
     l1:=lTag
     l2:=lTag.rest
     while l2 ¬ = [] repeat
       (ii:=l2.first.index) < m => return void()
       ii = m =>
         l1.rest:=l2.rest
         return void()
       l1:=l1.rest
       l2:=l2.rest
     void()

-- Pour tout remettre a zero avant un nouveau calcul
   clearAll == lTag.rest:=nil()$LRec

   lisTag() == [bouzins.index for bouzins in lTag.rest]

   coerce(f): E ==
     f.tag = [] => (f.val)::E
     f.val = 0 =>
       mkNary("+"::E, [sub(t) for t in f.tag])
     mkBinary("+"::E,(f.val)::E,
       mkNary("+"::E, [sub(t) for t in f.tag]))

   f = g ==
     f.val = g.val =>
       f.tag =$Tag g.tag => true
       false
     false

   0 == [0$Mon,[]]

   purTag?(f) == f.val = 0

   eval1(lrec:Tag):Mon ==
     resu:Mon:= 0
     for term in lrec repeat
       resu:=resu + term.exp * getVal(term.gen)
     resu

   eval(f:$):Mon ==
     f.val + eval1(f.tag)

   f + g ==
     [f.val + g.val,plus(f.tag,g.tag)]

   f - g ==
     (momo:= f.val - g.val) case "failed" => "failed"
     (tata:= moins(f.tag, g.tag)) case "failed" => "failed"
     [momo::Mon,tata::Tag]

   n * f ==
```

```
        [n * f.val, mult(n, f.tag)]

  -- On commence par trier en evaluant,
  -- puis en comparant les parties "en x",
  -- enfin on rafine par l'ordre lexicographique inverse.
     f < g ==
        eval(f) < eval(g) => true
        eval(f) > eval(g) => false
        f.val < g.val => true
        f.val > g.val => false
        less(f.tag, g.tag) => true
        false

     min(f,g) ==
        f < g => f
        g


     max(f,g) ==
        g < f => f
        g

     sup(f,g) == [sup(f.val,g.val),sup1(f.tag,g.tag)]
```

2. STANDMON

Ce package implante le calcul de la base standard d'un idéal monomial, qui est une sorte de "base standard de monoïde". L'algorithme utilisé est celui de Gebauer et Moeller du domaine public de Scratchpad II, simplifié pour la circonstance.

```
)abb package STANDMON StandardBasisForMonoid

StandardBasisForMonoid(Mon): Exportation == Production where

    Mon: OrderedAbelianMonoidSup
    NNI ==> NonNegativeInteger
    I ==> Integer
    E ==> Expression
    L ==> List
    MOFAM ==> MutableOrderedFreeAbelianMonoid(Mon)
    Prod ==> Record(fir:MOFAM,sec:MOFAM)
    Syz ==> Record(ltij:MOFAM,eli:Prod,elj:Prod)
    LREC ==> L Record(gen: I, exp: NNI)
    OUT ==> OutputPackage

    Exportation == with
    -- fonctions principales
       begin: (L Mon,Mon) -> L LREC
       continue: (Mon, I) -> L LREC
       exprime: Mon -> LREC
    -- fonctions annexes
       cont: () -> L LREC
       isRed1: L LREC -> I
       isRed: Prod -> Boolean
```

```
  evSyz: Syz − > Prod
  red1: (MOFAM,Prod) − > MOFAM
  red: MOFAM − > MOFAM
  reduire: Prod − > Prod
  genListSyz: () − > Void
  actualiseListSyz: Prod − > L Syz
  genBaseStan: () − > Void
  actualiseBaseStan: Prod − > L Prod
  nettoieBaseStan: L I − > L Prod
  redMemberP: (Prod, Prod) − > MOFAM
  redMemberS: (Syz, Prod) − > MOFAM
  nettoieListSyz: L I − > L Syz
  abs: (Prod,L Prod) − > L Prod
  abs2: (MOFAM, L Prod) − > L Prod
  mkProd: (Mon, I) − > Prod
  crit1: (Prod, Prod) − > Boolean
  crit2: (Syz, Syz) − > Boolean
  crit3: (Syz, Prod) − > Boolean
  appliqueCrit2:(Syz, L Syz) − > L Syz
  appliqueCrit3:(L Syz, Prod) − > L Syz
  merge: (L Syz, L Syz) − > L Syz
  nEv: () − > I

Production == add
-- Types
-- Variables globales
  zerProd:Prod:=[0$MOFAM,0$MOFAM]$Prod
  LProd:= L Prod
  baseStan: LProd:=[zerProd] -- avec une fausse tete
  LSyz:= L Syz
  listSyz:LSyz:=
    [[0$MOFAM,zerProd,zerProd]$Syz] -- avec une fausse tete
  nEvit:L I:=[0]
  monMax:L Mon:=[0]

-- Pour commencer un calcul de base standard
  begin(lmon,mon) ==
    monMax.0:= mon
    nEvit.0:=0
    clearAll()$MOFAM
    leq:L Prod:= []
    num:I:=£ lmon
    for mon in lmon repeat
      leq:=cons(mkProd(mon,num),leq)
      num:=num − 1
    leq:= sort(leq, £ 1.fir > £ 2.fir)
    baseStan.rest:=[leq.first]
    listSyz.rest:=nil()$LSyz
    for eq in leq.rest repeat
      actualiseListSyz(eq)
      actualiseBaseStan(eq)
    cont()


-- Utilise par BASECAN pour reprendre le calcul de la base standard
-- en rajoutant eventuellement un generateur
  continue(mon, i) ==
    if i ¬ = 0 then
      eq:= mkProd(mon, i)
```

```
      actualiseListSyz(eq)
      actualiseBaseStan(eq)
    cont()

  mkProd(mon, i) == [coev(mon)$MOFAM, new(i, mon)$MOFAM]$Prod

  redMemberS(syz,redu) ==
    syz.eli.sec:= red1(syz.eli.sec,redu)
    syz.elj.sec:= red1(syz.elj.sec,redu)

  redMemberP(eq,redu) ==
    eq.sec:= red1(eq.sec,redu)

-- Pour continuer le calcul de base standard
  cont() ==
    while (tls:=listSyz.rest) ¬ = [] repeat
      tlsf:=tls.first
      if monMax.0 ¬ = 0 then
        -- s'il n'y a plus de superposition
        eval tlsf.ltij > monMax.0 => return []
      eq1:= evSyz tlsf
      listSyz.rest:= tls.rest
      (redu:=reduire eq1).fir = 0 => "au suivant"
      actualiseListSyz(redu)
      actualiseBaseStan(redu)
      stan:=baseStan.rest
      purTag? redu.fir =>
        purTag? tlsf.ltij =>
          nEvit.0:= nEvit.0 + 1
        -- retourne une superpositio a BASECAN
        return [getTag redu.fir,getTag redu.sec]
    []

  isRed1(sup) ==
    l1:=sup.0
    £ l1 = 1 and l1.first.exp = 1 => l1.first.gen
    0

  isRed(redu) ==
    purTag? redu.fir and _
    isRed1 [getTag redu.fir, getTag redu.sec] ¬ = 0

  evSyz(syz) ==
    ele1:= (syz.ltij - syz.eli.fir)::MOFAM + syz.eli.sec
    ele2:= (syz.ltij - syz.elj.fir)::MOFAM + syz.elj.sec
    ele1 = ele2 => zerProd
    ele1 < ele2 => [ele2, ele1]$Prod
    [ele1, ele2]$Prod

  red1(mof,eq1) ==
    mof2:= eq1.fir
    mof3:= eq1.sec
    while (diff:= mof - mof2) case MOFAM repeat
      mof:= mof3 + diff::MOFAM
    mof

  red(mof) ==
    st:=baseStan.rest
    omof:=0$MOFAM
```

```
  while mof ¬ = omof repeat
    omof:=mof
    for eq1 in st repeat  mof:= red1(mof,eq1)
  mof

reduire(eq) ==
  (mof:= eq.fir) = (mof2:= eq.sec) => zerProd
  (nmof:=red mof) = mof2 => zerProd
  nmof > mof2 => [nmof, red mof2]
  reduire [mof2, nmof]

actualiseBaseStan(redu) ==
  stan:=baseStan.rest
  baseStan.rest:=abs(redu,baseStan.rest)

abs(redu,std) ==
  std = [] => [redu]
  std.first.fir < redu.fir => cons(std.first,abs(redu,std.rest))
  cons(redu,abs2(redu.fir,std))

abs2(firredu,std) ==
  std = [] => std
  std.first.fir − firredu case MOFAM  => abs2(firredu,std.rest)
  cons(std.first,abs2(firredu,std.rest))


actualiseListSyz(redu) ==
  lS:=listSyz.rest
  std:=baseStan.rest
  newSyz:L Syz:=
    [[sup(x.fir,redu.fir),x,redu]$Syz_
                                  for x in std — crit1(x,redu)]
  if newSyz ¬ = [] then
    sort(newSyz,£ 1.ltij < £ 2.ltij)
    newSyz:=appliqueCrit2(newSyz.first,newSyz.rest)
  lS:=appliqueCrit3(lS,redu)
  listSyz.rest:=merge(newSyz,lS)

crit1(eq1,eq2) ==
  sup(eq1.fir,eq2.fir) = eq1.fir + eq2.fir  => false
  true

crit2(syz1,syz2) == syz1.ltij − syz2.ltij case "failed"

crit3(syz,eq) ==
  (eq1:= syz.ltij) − eq.fir case "failed" or _
   sup(syz.eli.fir, eq.fir) = eq1 or sup(syz.elj.fir, eq.fir) = eq1

appliqueCrit2(syz,lS) ==
  lS:=[sy for sy in lS — crit2(sy,syz)]
  lS = [] => [syz]
  cons(syz,appliqueCrit2(lS.first,lS.rest))

appliqueCrit3(lS,redu) == [sy for sy in lS — crit3(sy,redu)]

merge(lS1,lS2) ==
  lS1 = [] => lS2
  lS2 = [] => lS1
  (s1:= lS1.first).ltij < (s2:= lS2.first).ltij =>
```

```
        cons(s1,merge(lS1.rest, lS2))
      cons(s2,merge(lS1, lS2.rest))

-- utilise par BASECAN pour la reduction
-- decompose un monome en un produit des monomes de tete
-- si c'est possible, sinon retourne la liste vide
   exprime(mon) ==
      mof:= coev mon
      purTag? (mof:= red mof) => getTag mof
      []

   nEv() == nEvit.0
```

3. BASECAN

Ce package implante le calcul de la base canonique.

```
-- Address comments and questions to
--   François OLLIVIER
--   Laboratoire d'Informatique de L'X (LIX)
--   Ecole Polytechnique
--   91 128 Palaiseau cedex (FRANCE)
--   BITNET: CFFOLL@FRPOLY11

-- This domain implements a completion procedure for building the
-- canonical basis of a k-subalgebra of k[x1,...xn]. A canonical basis
-- plays the same role for k-subalgebras as standard basis for ideals.
-- The degrees (according to the degree function of spad) of polynomials
-- in the C.B. form a minimal set of generators for the submonoid of
-- N**n consisting of the degrees of all polynomials in the subalgebra.
-- Unfortunately, the C.B. could be infinite, so that the completion
-- procedure never stops. It must be said that, in our implementation,
-- the completion procedure may never stop, even if the C. B. is finite
-- except for degree orderings (which means all orderings sorting
-- polynomials at first according to their total degree). This is
-- no great limitation, for the degree ordering (implemented in NDMP)
-- works well.

-- BaseCanonique takes 1, 2 or 3 arg. The first is a list of polynomials
-- the second a list of string which can be "trace", "info" or
-- "relations".
-- "info" displays the set of polynomials calculated after each
-- reduction.
-- "trace" allows the user to obtain the trace of calculations, and so
-- the expression of pols in the C.B. in function of generating pols.
-- For that issue playBack() after having computed the C.B.
-- "relations" allows the user to get relations between pols in the C.B.
-- For that issue baseStandard after calculating the C.B. (the given
-- polynomials form a standard basis for some order).
-- The third arg is a pol, no superposition will be computed if its
-- degree is greater that the degree of that pol, exept if it is 0
-- We consider the multidegree with current ordering (not totalDegree
-- which is unfortunately not implemented!?).
-- reduire gives the reduction of a pol with respect to the C.B. It is 0
-- iff the pols belongs to the subalgebra.
-- reduireExpr gives the reduction and its expression from pols in the
```

```
-- C.B.
-- Nota: pols in the C.B. are numered according to their order of
-- appearance. Issue getPol(n) to know which has number n.
--
-- For using this you need MOFAM, which represent a monoid, and
-- STANDMON, which calculates Standard basis on a monoid in order to
-- find superpositions.

-- % BaseCanonique
)abb package BASECAN BaseCanonique

BaseCanonique(k,kAlg,Mon): Exportation == Production where
   k: Field
   Mon: OrderedAbelianMonoidSup
   kAlg: GeneralPolynomial(k,Mon)
   Pol ==> Polynomial k
   I ==> Integer
   NNI ==> NonNegativeInteger
   E ==> Expression
   SE ==> SortedExpressions
   S ==> String
   L ==> List
   MOFAM ==> MutableOrderedFreeAbelianMonoid Mon
   STAND ==> StandardBasisForMonoid Mon
   REC ==> Record(gen: I, exp: NNI)
   LREC ==> L Record(gen: I, exp: NNI)
   RecTrace ==> Record(index: I, sup: L LREC)
   RecExpr ==> Record(index:I, exp: Pol)
   RecRed ==> Record(po: kAlg, exp: Pol)
   OUT ==> OutputPackage


   Exportation == with
      baseCanonique: L kAlg -> L kAlg
      baseCanonique: (L kAlg, L S) -> L kAlg
      baseCanonique: (L kAlg, L S, kAlg) -> L kAlg
      reduire: kAlg -> kAlg
      reduireExpr: kAlg -> RecRed
      baseStandard: () -> L Pol
      playBack: () -> L RecExpr
   -- fonctions annexes (destinees a devenir locales)
      conforme: (L I, L LREC) -> Boolean
      reduire2: RecRed -> RecRed
      getPol: I -> kAlg
      mkMonic: kAlg -> I
      mkMonic2: RecRed -> Pol
      delConst: kAlg -> kAlg
      eval: LREC -> kAlg
      calcSup: L LREC -> I
      calcSup2: L LREC -> Pol
      calcSup3: L LREC -> Pol
      num: () -> I
      delPol: I -> I
      redReductum: kAlg -> kAlg
      redReductum2: RecExpr -> RecExpr
      formExpr: LREC -> Pol
      findRecExpr: (L RecExpr, I) -> RecExpr
```

```
Production == add
-- variables globales
  numPols:L I:=[0]
  nR0:L I:=[0]
  registre:= Record(index: I,member: kAlg)
  LReg:= L registre
  listPols:L registre:= [[0,0]$registre] -- avec une fausse tete
  saveBaseCan:L kAlg:= [0$kAlg] -- idem
  listTrace:L RecTrace:= [[0,nil()$L(LREC)]$RecTrace] -- idem
  listRelat:L L LREC:= [nil()$L(LREC)] -- idem
  savePols:L kAlg:= [0] -- idem
  string1:S:= "Nombre de superpositions reduites a 0 :"
  string2:S:= "Nombre de superpositions evitees par le critere 3 :"
  sTr:S:= "trace"
  sInf:S:= "info"
  sRel:S:= "relations"
  flagI:L Boolean:= [false]
  flagT:L Boolean:= [false]
  flagR:L Boolean:= [false]
  maxDeg:L Mon:= [0]
  monMax:L Mon:= [0]


-- implantation des fonctions principales
  baseCanonique(lpol) == baseCanonique(lpol,[],0)

  baseCanonique(lpol,lst) == baseCanonique(lpol,lst,0)

  baseCanonique(lpol,lst,pdm) ==
    monMax.0:= (mon:= degree pdm)
    nR0.0:= 0
    numPols.0:=0
    listPols.rest:=nil()$LReg
    listTrace.rest:=nil()$L(RecTrace)
    listRelat.rest:=nil()$L(L(LREC))
    if member(sInf,lst) then flagI.0:= true
      else flagI.0:= false
    if member(sTr,lst) then flagT.0:= true
      else flagT.0:= false
    if member(sRel,lst) then flagR.0:= true
      else flagR.0:= false
  -- et non pas  :=[] comme on penserait pouvoir l'ecrire...
    lpol:=sort(lpol,degree £ 1 > degree £ 2)
    if flagT.0 then savePols.rest:= lpol
    for pol in lpol repeat mkMonic delConst pol
    -- initialise le calcul de la base standard
    superposition:L LREC:=
      begin([degree reg.member for reg in listPols.rest], mon)$STAND
    -- boucle principale
    while superposition ¬ = [] repeat
      -- a chaque superposition,
      i:= calcSup superposition
      if i = 0 then
          nR0.0:= nR0.0 + 1
          if flagR.0 then listRelat.rest:=
            cons(superposition,listRelat.rest)
        else if flagT.0 then
          listTrace.rest:=
            cons([i, superposition]$RecTrace, listTrace.rest)
```

```
      -- si c'est la reduction d'un polynome, on le supprime
      delPol isRed1(superposition)$STAND
      if flagI.0 then
         baseCan:=[reg.member for reg in listPols.rest]
         output(baseCan::E)$OUT
      -- on itere le calcul de la base standard
      -- pour chercher une nouvelle superposition
      superposition:=continue(degree getPol i, i)$STAND
   baseCan:=
      [(reg.member:=redReductum reg.member) for reg in listPols.rest]
   if flagT.0 then listTrace.rest:= nreverse listTrace.rest
   if flagI.0 then
      output(string1, (nR0.0)::E)$OUT
      output(string2, (nEv()$STAND)::E)$OUT
      if flagT.0 then output((listTrace.rest)::E)$OUT
   baseCan:= sort(baseCan, degree £ 1 < degree £ 2)
   if flagR.0 then saveBaseCan.rest:= baseCan
   baseCan


-- Pour reduire un polynome par la base canonique
 reduire pol ==
   pol = 0 => 0
   lrec:= exprime(degree pol)$STAND
   lrec ¬ = [] => reduire (pol − lc pol * eval lrec)
   monom(degree pol, lc pol) + reduire red pol

-- pour le reduire en calculant son expression en fonction des generateurs
 reduireExpr pol ==
   recred:=reduire2 [pol,0]$RecRed
   recred.exp:= −recred.exp
   recred

-- Calcul d'une base standard de l'ideal des relations
 baseStandard() ==
   ¬ flagR.0 => error "use baseCanonique with string:= relations—"
   listPols.rest:=nil()
   numPols.0:=0
   lpol:= reverse saveBaseCan.rest
   for pol in lpol repeat mkMonic pol
   superposition:L LREC:=
      begin([degree pol for pol in saveBaseCan.rest], monMax.0)$STAND
   lRel:L Pol:= []
   -- On reduit toutes les superpositions
   while superposition ¬ = [] repeat
      -- On recupere la liste des relations evidentes
      lRel:= cons(calcSup3 superposition, lRel)
      superposition:= continue(0$Mon,0$I)$STAND
   nreverse lRel

-- Reprend le calcul de la base canonique
-- et exprime les polynomes de la base en fonction des generateurs
 playBack() ==
   ¬ flagT.0 => error "Sorry boy, there's nothing to play back—"
   numPols.0:=0
   listPols.rest:=nil()$LReg
   pb:L(RecExpr):=[]
   lpol:= [pol for pol in savePols.rest — degree pol > 0]
   numer:=£ lpol
```

```
      for pol in lpol for i in 1..numer repeat
        expr:Pol:=
          expr1:= varPol(mkBinary("SUB","p",i::E)::SE)
          (expr1 - coef(pol,0)::Pol) / lc pol
        pb:=cons([i,expr],pb)
      for pol in lpol repeat mkMonic delConst pol
      lpol2:=reverse lpol
      superposition:L LREC:=
        begin([degree pol for pol in lpol2], monMax.0)$STAND
      for tra in listTrace.rest repeat
        j:I:= tra.index
        while superposition ¬ = tra.sup repeat
          delPol isRed1(superposition)$STAND
          superposition:=continue(0$Mon, 0$I)$STAND
        pb:=cons([j, calcSup2 tra.sup],pb)
        delPol isRed1(superposition)$STAND
        baseCan:=[reg.member for reg in listPols.rest]
        output(baseCan::E)$OUT
        superposition:=continue(degree getPol j, j)$STAND
      while superposition ¬ = [] repeat
        delPol isRed1(superposition)$STAND
        superposition:=continue(0$Mon, 0$I)$STAND
      for reg in listPols.rest repeat
        redReductum2 findRecExpr(pb, reg.index)
      nreverse pb

-- implantation des fonctions annexes
    conforme(lind,super) ==
      for lrec in super repeat
        for rec in lrec repeat
          ¬ member(rec.gen,lind) => return false
      true

    reduire2 polExpr  ==
      pol:= polExpr.po
      expr:= polExpr.exp
      pol = 0 => polExpr
      lrec:= exprime(degree pol)$STAND
      lrec ¬ = [] =>
        expr:= expr - lc pol * formExpr lrec
        reduire2 [pol - lc pol * eval lrec, expr]$RecRed
      [monom(degree pol, lc pol) +_
        (suite:= reduire2 [red pol,expr]$RecRed).po, suite.exp]$RecRed

-- Rend le reste de la reduction unitaire et complete la base
-- canonique s'il est non nul. Retourne l'indice du nouveau polynome.
    mkMonic(pol) ==
      pol = 0 => 0
      listPols.rest:=
        reg:=[numPols.0 := numPols.0 + 1, pol / lc pol]$registre
        cons(reg,listPols.rest)
      numPols.0

    mkMonic2(polexpr) ==
      pol:= polexpr.po
      expr:= polexpr.exp
      expr:= expr / lc pol
      listPols.rest:=
        reg:=[numPols.0 := numPols.0 + 1, pol / lc pol]$registre
```

```
      cons(reg,listPols.rest)
    expr

  getPol(i) ==
    i = 0 => 0
    listP:=listPols.rest
    for reg in listP repeat
      reg.index = i => return reg.member
    error "can't find it"

  delPol(j) ==
    j = 0 => j
    listP:=listPols
    while listP.rest ¬ = [] repeat
      if listP.rest.first.index = j then
        polreduit:=listP.rest.first.member
        listP.rest:= listP.rest.rest
        return j
      listP:=listP.rest
    error "can't find it"

  num() == numPols.0

  eval(lrec) ==
    pol:= 1$kAlg
    for rec in lrec repeat
      pol:= pol * getPol(rec.gen)**(rec.exp)
    pol

  delConst(pol) == pol - coef(pol,0$Mon)::kAlg

  formExpr lrec ==
    resExpr:= 1$Pol
    for rec in lrec repeat
      resExpr:= resExpr *_
         varPol(mkBinary("SUB"::E,"p"::E,(rec.gen)::E)::SE)**rec.exp
    resExpr

-- Reduit le S-polynome associe a une superposition.
  calcSup(llrec) ==
    pol1:= eval llrec.0
    pol2:= eval llrec.1
    mkMonic reduire (pol1 - pol2)

  calcSup2 llrec ==
    pol1:= eval llrec.0
    pol2:= eval llrec.1
    expr:Pol:= formExpr llrec.0 - formExpr llrec.1
    mkMonic2 reduire2 [pol1 - pol2, expr]$RecRed

-- Calcule la relation evidente associee a une superposition
  calcSup3 llrec ==
    pol1:= eval llrec.0
    pol2:= eval llrec.1
    expr:Pol:= formExpr llrec.0 - formExpr llrec.1
    (reduire2 [pol1 - pol2, expr]$RecRed).exp

  redReductum pol ==
    monom(degree pol, lc pol) + reduire red pol
```

```
redReductum2 recexpr ==
   expression:= recexpr.exp
   i:= recexpr.index
   recexpr.exp:= reduire2([red getPol(i),expression]$RecRed).exp
   recexpr

findRecExpr(pb,i) ==
   for recexpr in pb repeat
      recexpr.index = i => return recexpr
   error "can't find it"
```

Références bibliographiques

[AB] K. ADJAMAGBO et P. BOURY, *A resultant criterion and formula for the inversion of a polynomial map in two variables*, prépublication ENPC, CERMA, Noisy-le-Grand, 1989.

[AM] S. S. ABHYANKAR et T.-T. MOH, *Embeddings of the Line in the Plane*, J. Reine Angew. Math. 276, 149–166, 1975.

[BA] N. BOURBAKI, *Algèbre*, chap. 4–7, Masson, Paris, 1981.

[BCW] H. BASS, E. H. CONNELL et D. WRIGHT, *The Jacobian Conjecture: Reduction of Degree and Formal Expansion of the Inverse*, Bull. A.M.S., vol. 7, n° 2, 287-330, 1982.

[Bel] R. BELLMAN et K.J. ÅSTRÖM, *On structural identifiability*, Math. Biosci., 7, 329–339, 1970.

[Bu1] B. BUCHBERGER, *A Criterion for Detecting Unnecessary Reductions in the Construction of Groebner Bases*, Actes de EUROSAM79, Marseille, Lect. Notes in Comp. Science 72, 2–31, Springer Verlag, Juin 1979.

[Bu2] B. BUCHBERGER, *Groebner Bases: an Algorithmic Method in Polynomial Ideal Theory*, Multidimensional Systems Theory, N. K. Bose éditeur, Reidel, 184–232, 1985.

[Car1] G. CARRA'-FERRO, *Gröbner bases and differential ideals*, actes de AAECC5, Menorca, Spain, 129–140, Springer Verlag, Juin 1987.

[Car2] G. CARRA'-FERRO, *Kolchin Schemes*, Journal of Pure and Applied Algebra 63, 13–27, North-Holland, 1990.

[Car3] G. CARRA'-FERRO, *On Term-Orderings and Ranking*, Informal session, MEGA'90.

[Cas] F. CASTRO, *Théorème de division pour les opérateurs différentiels et calcul des multiplicités*, thèse de troisième cycle, Paris VII, Oct. 1984.

[CT] P. CONTI et C. TRAVERSO, *Computing the Conductor of an Integral Extension*, preprint, 1989.

[De] R. DESNOS, *Corps et biens*, N.R.F., Paris, 1930.

[DD] C. DICRESCENZO et D. DUVAL, *Algebraic Computation on Algebraic Numbers*, Computers and Computing, Chenin et al. éd., 54–61, Masson et Whiley, 1985.

[Di] S. DIOP, *Théorie de l'élimination et principe du modèle interne en automatique*, thèse de doctorat en science, Univ. Paris Sud, 1989.

[Du] D. DUVAL, *Computation with Algebraic Numbers: the D5 Method*, soumis à J. Symb. Comp., 1989.

[E] A. VAN DEN ESSEN, *A criterion to decide if a polynomial map is invertible and to compute the inverse*, report 8653, Catholic University Nijmegen, Pays-Bas, 1986.

[FGLM] J.C. FAUGÈRE, P. GIANNI, D. LAZARD and T. MORA, *Efficient computation of zero-dimensional standard bases by change of ordering*, preprint 1988.

[FGM] N. FITCHAS, A. GALLIGO, J. MORGENSTERN, *Precise sequential and parallel complexity for quantifier elimination over algebraically closed fields*, à paraître dans Journal of Pure and Applied Algebra, 1987.

[Fl] M. FLIESS, *Automatique et corps différentiels*, Forum Math., 1, 1989.

[Gal] A. GALLIGO, *Somme algorithmic questions on ideals of differential operators*, actes d'EUROCAL'85, vol. II, 413–421, Lect. Notes in Comp. Science, Springer, 1985.

[God] L. GODEAUX, *Les transformations birationnelles du plan*, Gauthier-Villars, Paris, 1927.

[Ha] R. HARTSHORNE, *Algebraic Geometry*, Springer, 1977.

[Hu] G. HUET, *An Algorithm to Generate the Basis of Solutions to Homogeneous Linear Diophantine Equations*, Information Processing Letters, 7, 3, 144-147, 1978.

[Ja] M. JANET, *Systèmes d'équations aux dérivées partielles*, J. de Math., 8e série, tome III, 1920.

[Jo] J.-P. JOUANOLOU, *Monoïdes*, publ. IRMA 297/P-162, Strasbourg, 1984.

[Ju] H.W.E. JUNG, *Über ganze birationale Transformationen des Ebene*, J. Reine Angew. Math., 184, 161–174, 1942.

[KM] D. KAPUR et K. MADLENER, *A Completion Procedure for Computing a Canonical Basis of a k-Subalgebra*, Computers and Math., E. Kaltofen et S. M. Watt éditeurs, Springer, 1989.

[Ko1] E. R. KOLCHIN, *Galois Theory of Differential Fields*, Amer. J. Math., 75, 753-824, 1953.

[Ko2] E. R. KOLCHIN, *Differential Algebra and Algebraic Groups*, Academic Press, New-York, 1973.

[Kol] J. KOLLÁR, *Sharp Effective Nullstellensatz*, J. Am. Math. Soc., 1, 963–975, 1988.

[Ku] W. van der KULK, *On Polynomial Rings in two Variables*, Nieuw. Arch. Wiskunde 1, 33-41, 1953.

[La] D. Lazard, *A New Method for Solving algebraic systems of positive dimension*, prépublication du LITP, Paris VII, n° 89-77, conférence invitée à AAECC'7, Toulouse, 1989.

[Le] Y. LECOURTIER, *Propriétés structurelles de modèles : études théoriques, tests formels, applications à la catalyse hétérogène*, Thèse de Doctorat ès Sciences, Université Paris-Sud, 1985.

[LLW] Y. LECOURTIER, F. LAMNABHI-LAGUARRIGUE, et E. WALTER, *A Method to Prove that Non-Linear Models can be Unidentifiable*, actes de 26th Conference on Decision and Control, Los Angeles, CA, 2144–2145, Décembre 1987.

[Lev] H. LEVI, *On the structure of differential polynomials and on their theory of ideals*, Transactions of the A.M.S., vol 51, 326–365, 1942.

[M] Yu. I. MANIN, *Rational Surfaces over Perfect Fields II*, Math. USSR-Sb., 1, 141-168, 1967.

[MM] E. W. MAYR et A. MEYER, *The Complexity of the Word Problem for Commutative Semigroup and Polynomials Ideals*, Advances in Math., 46, 305–329, 1982.

[Moh] T.-T. MOH, *On the Jacobian conjecture and the configuration of roots*, Journal für Math., 340, 140–212, 1982.

[Mol] H. M. MOELER, *A reduction strategy for the taylor resolution*, actes de EUROCAL'85, Linz, 1985.

[N] M. NAGATA, *On the Automorphism Group of* $k[x, y]$, Lect. Math. Kyoto University, 1972.

[O1] F. OLLIVIER, *Inversibility of rational mappings and structural identifiability in automatics*, actes de ISSAC'89, Portland Oregon, 43–53, ACM Press, 1989.

[O2] F. OLLIVIER, *Canonical bases: relations with standard bases, finiteness conditions and application to tame automorphisms*, à paraître dans les actes de MEGA'90, Castiglioncello, Birkhauser, 1990.

[O3] F. OLLIVIER, *Standard Bases of differential ideals*, soumis à AAECC'8, Tôkyô, 1990.

[Po1] J.-F. POMMARET , *Systems of partial differential equations and Lie pseudogroups*, Gordon and Breach, New-York, 1978.

[Po2] J.-F. POMMARET, *Differential Galois theory*, Gordon and Breach, New-York, 1983.

[Po3] J.-F. POMMARET, *Lie pseudogroups ans mechanics*, Gordon and Breach, New-York, 1988.

[Po4] J.-F. POMMARET, *Effective methods for systems of algebraic partial differential equations*, présenté à MEGA'90, Castiglioncello, 1990.

[Ra] A. RAKSANYI, *Utilisation du calcul formel pour l'étude des systèmes d'équations polynomiales (Applications en modélisation)*, thèse de troisième cycle, Université Paris-Dauphine, 1986.

[Riq] RIQUIER, *Les systèmes d'équations aux dérivées partielles*, Gauthier-Villars, Paris, 1910.

[Ri1] J.F. RITT, *Differential Equations from the Algebraic Standpoint*, Amer. Math. Soc. Colloq. Publ., vol. 14, A.M.S., New-York, 1932.

[Ri2] J.F. RITT, *Differential algebra*, Amer. Math. Soc. Colloq. Publ., vol. 33, A.M.S., New-York, 1950.

[Ro1] L. ROBBIANO, *Terms ordering on the polynomial ring*, actes de EUROCAL'85, vol. II, 513–517, 1985.

[Ro2] L. ROBBIANO, *On the Theory of Graded Structures*, J. Symb. Comp. 2, 1986.

[RS] L. ROBBIANO et M. SWEEDLER, *Subalgebra Bases*, preprint, Cornell Univ., 1989.

[Scr] R. S. SUTOR éd., *The Scratchpad Computer Algebra System Interactive Environment Users Guide*, Computer Algebra Group, Math. Sciences Dep., IBM Research Division, Thomas J. Watson Research Center, Yorktown Heights, 25 Octobre 1989.

[Se] B. SEGRE, *Forme differenziali e loro integrali*, vol. II, Docet, Rome, 1956.

[Sei] A. SEIDENBERG, *An elimination theory for differential algebra*, Univ. California Publications in math., (N.S.), 3, n°2, 31–65, 1956.

[SS] D SHANNON et M. SWEEDLER, *Using Groebner Bases to Determine Algebra Membership, Split Surjective Algebra Homomorphisms and Determine Birational Equivalence*, preprint 1987, paru dans J. Symb. Comp., 6, 2–3.

[Sw] M. SWEEDLER, *Ideal bases and valuation rings*, preprint, 1988.

[Th] J. M. THOMAS, *Systems and Roots*, W. Byrd Press, Richmond (Virginia), 1962.

[V] V. VYSOTSKIĬ, *Nerv*, (en russe), Sovremennik, Moskva, 1981.

[Wa1] E. WALTER, *Identifiability of State Space Models*, Lect. notes in Biomath. n° 46, Springer 1982.

[Wa2] Collectif : DISTEFANO, LAMNABHI-LAGUARRIGUE, LECOURTIER, RAKSANYI, VAJDA, WALTER, etc..., *Identifiability of parametric models*, E. Walter éditeur, Pergamon Press, Oxford, 1987.

[WL] E. WALTER et Y. LECOURTIER, *Global approches to identifiability testing for linear and non-linear state space models*, Mathematics and computers in Simulation, XXIV, 472–482, 1982.

[Wu1] WU W.-T., *A Zero Structure Theorem for Polynomial Equation Solving*, Math.-Mechanization Research Preprints 1, 2–12, Academia Sinica, Beijing, 1987.

[Wu1] WU W.-T., *A Zero Structure Theorem for Polynomial Equation Solving and its applications*, actes de ISSAC'88, Rome, Italie, Springer Verlag, 1988.

[ZS] O. ZARISKI et P. SAMUEL, *Commutative Algebra*, vol I, Springer Verlag, 1958.

Index des notations

Certaines notations sont utilisées dans différents domaines avec des significations distinctes. Dans la mesure où elles interviennent dans des parties indépendantes du texte, il était cependant commode de les utiliser avec un sens dépendant du contexte. Les notations "locales" figurent avec la partie du texte concernée entre crochet : [chap. III § 1], par exemple.

Index terminologique

Table des matières