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 $M = \prod_{i=1}^{r} \upsilon_i^{\alpha_i}$ and $M' = \prod_{i=1}^{s} \nu_i^{\beta_i}$, where the υ_i and ν_i appear in strictly decreasing order. We take $M < M'$ if there exist $j \leq r, s$ such that $\upsilon_i = \nu_i$ $i < j$, $\alpha_i = \beta_i$ $i < j$, $\upsilon_j < \nu_j$ or $\upsilon_j = \nu_j$ 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 $\delta\, m = \delta\, \upsilon_1\, \upsilon_1^{\alpha_1 - 1} \prod_{i=2}^{r} \upsilon_i^{\alpha_i}$. 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 υ be the leading derivative of M_i for $i > r$. The degree in υ 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 υ^d, for $i \geq s$, we secure a new strictly decreasing sequence of monomials, whose leading derivatives are smaller than υ. 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 $P \xrightarrow{\Sigma^*} R$.

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. — *$P \xrightarrow{\Sigma^*} 0$, 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 $P \xrightarrow{\Sigma^\star} R$ 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 $Q \backslash$m P => return reduction$(P - (\mathrm{lc}\, P/\mathrm{lc}\, Q)\,(\mathrm{m}\, P/\mathrm{m}\, Q)\, Q, Q)$
  for $i \in [r, \ldots, m]$ repeat
    if $(P_2 :=$ reduction$(P, \delta_i\, Q, i)) \neq P$ then return reduction(P_2, 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 $P \xrightarrow{G^\star} 0$, 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 $x_{(r)}^s$ $s \leq q$. 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 $x_i - y_i$ $1 \le i \le n$.

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 $1 \le i \le n$ 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 $x_{i,(\theta)}^d$ l'élément $(d, x_{i,(\theta)})$ de $\mathbf{N} \times \Upsilon$. On étend à cet ensemble les dérivations de Δ en posant $\delta\, x_{i,(\theta)}^d = x_{i,(\delta\theta)}$. L'ordre de Υ est étendu en posant $v^d < \nu^e$ si $v < \nu$ ou si $v = \nu$ 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) $v^d \nu^e = v^d$ si $v > \nu$ et v^{d+e} si $v = \nu$,

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 $a1 = \top$ 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 $R = R_2 \upsilon_P^{\deg_P} + F$* 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 $P = 0 \Rightarrow Rec$
  $v_P = v_Q \Rightarrow$
    réduction1$([I_Q P - I_P v_P^{\deg Q - \deg P} Q, I_Q Rec.fact], Q)$
  $v_P = \theta\, v_Q \Rightarrow$
    réduction1$([S_Q P - I_P v_P^{\deg Q - 1} \theta\, Q, I_Q Rec.fact], Q)$
  $Rec1 :=$ réduction1$([I_P, 1], Q)$; $Rec2 :=$ réduction1$([Rec1.fact$ 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 $\mathrm{rg}P = v_P^d \theta \mathrm{rg}Q$, 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 v_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 $v_{f_i} < v_{f_j}$ $i < j$. On pose $v_C = \{x_1, \ldots, x_p, y_1, \ldots, y_q\}$, 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 $\{f_1, \dots, f_{q-1}\}$, 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 $\mathcal{J}' = \mathcal{J} \cap \mathcal{F}[x_1, \dots, x_p, y_1, \dots, y_{q-1}]$. Soit $(\eta_1, \dots, \eta_{p+q-1}, \epsilon)$ 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 $\{f_1, \dots, f_{q-1}\}$. 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 $\mathcal{R}$, $C = \{f_1, \dots, f_q\}$, où les f_i sont rangés par rang croissant, un sous-ensemble autoréduit et cohérent de $\mathcal{I}$. On note C_i l'ensemble $\{f_1, \dots, f_i\}$, C_0 sera $\{0\}$ par convention. On note à nouveau $x_1, \dots, x_p$ les dérivées intervenant dans les polynômes f_i, mais qui ne sont pas la dérivée dominante d'un des f_i et $y_1, \dots, y_q$, les dérivées dominantes des f_i. L'idéal $\mathcal{J}_i$ sera l'idéal engendré par C_i dans l'anneau $A_i = \mathcal{F}(x_1, \dots, x_p)[y_1, \dots, y_i]$.*

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 $\mathcal{I} \cap \mathcal{F}[x_1, \dots, x_p, y_1, \dots, y_q]$ est égal à $\mathcal{J} = (C) : H_C^\infty$. Soit P un polynôme de $\mathcal{I} \cap \mathcal{F}[x_1, \dots, x_p, y_1, \dots, y_q]$. 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 $pol \in lPol$ repeat
        if ($rest :=$réduction($pol, ensCar$)) $\neq 0$ then $L_1 :=$cons($rest, L_1$)
      for $sp \in$SPol($ensCar$) repeat
        if ($rest :=$ réduction($pol, ensCar$)) $\neq 0$ then $L_1 :=$cons($rest, L_1$)
      $lPol :=$append($L_1, lPol$)
    $flag :=$ false
    for $P \in ensCar$ repeat
      if $I_P \in \mathcal{I}$ then $flag :=$ true ; $lPol :=$ cons($I_P, lPol$)
      if $S_P \in \mathcal{I}$ then $flag :=$ true ; $lPol :=$ cons($S_P, lPol$)
      if ($inv :=$ inverse($I_P, ensCar$)) case Rec then
        $flag :=$ true
        if $inv.fact1 \in \mathcal{I}$ then $new := inv.fact1$ else $new := inv.fact2$
        $lPol :=$ cons($new, lPol$)
      if ($inv :=$ inverse($S_P, ensCar$)) case Rec then
        $flag :=$ true
        if $inv.fact1 \in \mathcal{I}$ then $new := inv.fact1$ else $new := inv.fact2$
        $lPol :=$ cons($new, lPol$)
  $ensCarNorm := [\,]$
  for $P \in ensCar$ 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 $\mathcal{J}$.