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 $\mathcal{B}'(A)$:

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

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

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

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 $B_a \subset B_b \iff a \leq b$.*

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 :*

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

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* $\mathrm{reste}(a) = a - \kappa(a)\mu \circ \tau a$ *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* $\mathrm{reste}\, a \xrightarrow{E} c$ *et* $b = \kappa a \mathrm{tête}\, a + c$. *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* $\mathrm{red}_D(a)$.

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

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 $\tau \mathrm{reste}\, b > \tau(b - c)$ et $\tau \mathrm{reste}\, c > \tau(b - c)$, $\tau \mathrm{reste}\, b = \tau \mathrm{reste}\, c$ et $\kappa \mathrm{reste}\, b = \kappa \mathrm{reste}\, c$. Par récurrence, on voit qu'il existe un entier i tel que $\tau \mathrm{reste}^{i+1}(b \text{ ou } c) \leq \tau(b - c)$, $\tau \mathrm{reste}^i b > \tau(b - c)$ et $\tau \mathrm{reste}^i c > \tau(b - c)$. Ceci implique $\tau \mathrm{reste}^{i+1}(b \text{ ou } c) = \tau(b - c)$ et donc b ou c réductible ; contradiction.

Pour la seconde partie, montrons d'abord que $B = D + V$. Soit $a \in B$, $a - \mathrm{red}_D(a) \in D$ et $\mathrm{red}_D a \in V$ 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 $\mathrm{unit}(\kappa(b)a - \kappa(a)b)$, *si* $a, b \neq 0$ *et* $\mathrm{unit}\, a$ *(resp.* $\mathrm{unit}\, b$*) 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 $[E]_{B'(A')}$ de rang inférieur où égal à r, et l'on pose $B_{r,n+1}(E) = B_{r,0}\big(B_{r,n}(E)\big)$. 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 $k(f_1,\dots,f_m)$ où $f_i = P_i/Q_i \in \mathrm{Fr}k[x_1,\dots,x_n]/\mathcal{I}$ ssi la base standard G de l'idéal*

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

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 $x_1,\dots,x_n$, 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 $A = k[P_1, \dots, P_m]$ 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 $g, f_1, \dots, f_m$ 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 $\widetilde{\text{graphe}}$ — et ne contient pas x_0. Pour tout $1 \leq i \leq n$, un polynôme de la forme $x_0^p(S_i(T)\widetilde{x_i} - R_i(x))$ 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, $\mathrm{Mon}E$ *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 $\operatorname{mdeg}\mathcal{I}$ (resp. $\operatorname{mdeg}A$) 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

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

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* 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*

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

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

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, $P \xrightarrow{C^\star} 0$.

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* $\{\text{mdeg}P | P \in I\}$ *of M. Then we say that a subset G of I is a standard basis of I if the set* $\{\text{mdeg}P | P \in G\}$ *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*

$$\text{mdeg}(m(P)Q) = \text{mdeg}(m'(P)R).$$

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* 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* $\mathrm{mdeg}P \in \overline{\mathcal{C}A}$*, 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* $\mathrm{Mon}A$*, 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 $\deg_p(y_i) = \mathrm{deg}P_i$, 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* $\mathrm{Mon}A$*, 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 $\mathcal{C}\{p, p'\} \cap$ 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

$$\frac{aD}{r}\left(\frac{\sigma+\varepsilon}{1+\sigma+\varepsilon} - \frac{\beta}{\alpha+\beta}\right) \sim \nu(aD) \geq H(aD) \geq \mu(aD) \sim \frac{aD}{r}\left(\frac{\sigma-\varepsilon}{1+\sigma-\varepsilon} - \frac{\beta}{\alpha+\beta}\right).$$

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

$$f : \begin{array}{ccc} x & \mapsto & x - 2y(y^2 + xz) - z(y^2 + xz)^2 \\ y & \mapsto & y + z(y^2 + xz) \\ z & \mapsto & z, \end{array}$$

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

$$\begin{array}{cccc} f: & \mathbf{C}^9 & \mapsto & \mathbf{C}^{12} \\ (x_{\ell,m}\ 1 \le \ell, m \le 3) & \mapsto & (S_{i,j,k}\ 1 \le i,j,k \le 3\ j,k \ne i), & \end{array}$$

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

$$\begin{array}{cccc} g\colon & \mathbf{A}^2 & \mapsto & \mathbf{A}^2 \\ & (x,y) & \mapsto & (y+x^3, y), \end{array}$$

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.