CHAPITRE II

Inversibilité et appartenance à un sous-corps

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

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

§ 1. APPLICATIONS POLYNOMIALES ET RATIONNELLES

1. Définitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Ordre et degré d'une application rationnelle

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

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

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

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

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

3. Composition et applications inversibles

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

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

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

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

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

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

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

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

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

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

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

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

4. Problèmes

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

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

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

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

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

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

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

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

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

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

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

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

1. Définitions. Structure

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

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

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

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

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

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

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

en coordonnées affines.

PREUVE. Voir [God] ou [M]. ∎

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

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

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

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

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

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

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

où $\sigma \in S_n$.

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

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

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

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

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

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

preuve. Voir [BCW]. ■

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

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

est de degré d^{n-1}.

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

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

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

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

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

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

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

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

preuve. Il suffit d'appliquer le théorème en utilisant la remarque 4. ■

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

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

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

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

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

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

où les f_i/g_i sont les fractions définissant f.

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

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

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

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

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

et que le degré projectif majore le degré affine. ∎

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Structure

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

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

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

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

PREUVE. Cf [Ku]. ∎

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

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

PREUVE. Voir [AM]. ∎

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

2. Caractérisation. Conjecture jacobienne

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

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

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

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

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

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

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

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

a) f est un automorphisme.

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

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

PREUVE. Voir [BCW]. ∎

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

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

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

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

§ 4. IDÉAUX ASSOCIÉS À UNE APPLICATION RATIONNELLE

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

1. Graphe

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

■

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

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

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

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

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

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

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

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

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

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

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

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

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

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

■

Ces deux lemmes immédiats impliquent le résultat suivant.

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

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

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

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

2. Idéal Δ associé à un sous-corps

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

On en déduit immédiatement le corollaire.

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

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

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

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

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

§ 5. IDÉAUX ASSOCIÉS À UNE SOUS-ALGÈBRE

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

---

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

1. Graphe

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

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

PREUVE. $\Longrightarrow$ est immédiat.

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

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

2. Idéal Σ

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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