MONIQUE LEJEUNE-JALABERT

Chapitre 2 Solutions des systèmes algébriques

Cours de l'institut Fourier, tome 19 (1984-1985), p. 53-90
<http://www.numdam.org/item?id=CIF_1984-1985__19__53_0>

Chapitre 2

SOLUTIONS DES SYSTEMES ALGEBRIQUES

1. Le cas où $\operatorname{rg}_k k[X_1,\ldots,X_n]/I < \infty$

Soit k un corps, $\overline{k}$ une clôture algébrique de k . Soit $f_1,\ldots,f_t \in k[X_1,\ldots,X_n]$, $f_i \neq 0$, $i = 1\cdots t$. On désigne par I (resp. $\overline{I}$) l'idéal engendré par $(f_1,\ldots,f_t)$ dans $k[X_1,\ldots,X_n]$ (resp. $\overline{k}[X_1,\ldots,X_n]$). Choisissant un ordre total sur $\mathbf{N}^n$ satisfaisant l'hypothèse I.1.1, les algorithmes I.3.5 et 3.8 nous ont permis de déterminer une base standard puis une base standard de cardinal minimal $(g_1,\ldots,g_s)$ de I et par suite $\exp I$ et $E(I)$. Ceci nous a permis de tester si $\operatorname{rg}_k k[X_1,\ldots,X_n]/I$ est fini puisque $\operatorname{rg}_k k[X_1,\ldots,X_n]/I = \sharp\mathbf{N}^n - \exp I$ (I.2.9). Nous avons remarqué également que $(g_1,\ldots,g_s)$ est encore une base standard de $\overline{I}$ et que $\exp I = \exp\overline{I}$ et $E(I) = E(\overline{I})$ (I.2.5) (ce qui implique le fait d'ailleurs évident que $\operatorname{rg}_k k[X_1,\ldots,X_n]/I = \operatorname{rg}_{\overline{k}} k[X_1,\ldots,X_n]/\overline{I}$). Nous supposons maintenant que ce rang est fini.

1.1. — Dans toute la suite de ce paragraphe, l'ordre total sur $\mathbf{N}^n$ avec lequel nous travaillons est *l'ordre lexicographique* .

1.2 REMARQUE. — Les conditions suivantes sont équivalentes :

i) $\operatorname{rg}_k k[X_1,\ldots,X_n]/I = 0$;

ii) $1 \in I$;

iii) $1 \in \overline{I}$.

Dans ces conditions le système $(f_1,\ldots,f_t)$ n'a pas de solutions.

1.3. UN PROCÉDÉ DE RÉSOLUTION. — Si maintenant $1 \leq \sharp\mathbf{N}^n - \exp I < \infty$, $\alpha = \sup\{d \in \mathbf{N}\ ,\ (0,0,\ldots,0,d) \notin \exp I\} < +\infty$ et $(0,0,\ldots,,0,\alpha+1) \in \exp I$. Nous allons d'abord montrer que $J = \{i\ ,\ i = 1\cdots s\ ,\ g_i \in k[X_n]\}$ se réduit à un seul élément i_0 et que $\deg g_{i_0} = \alpha + 1$. En effet, $\exp I = \cup_{i=1\cdots s} \exp g_i + \mathbf{N}^n$. Il existe donc $i \in 1\cdots s$ tel que $(0,0,\ldots,0,\alpha+1) \in \exp g_i + \mathbf{N}^n$. D'après I.1.1, i), $\exp g_i \leq (0,\ldots,\alpha+1)$ et l'ordre étant l'ordre lexicographique, il existe $\beta \in \mathbf{N}$, $\beta \leq \alpha + 1$ tel que $\exp g_i = (0,\ldots,0,\beta)$ et $g_i \in k[X_n]$ (I.4.1). J est donc $\neq \emptyset$. Mais $(g_1,\ldots,g_s)$ étant une base standard minimale, J ne peut contenir plus d'un élément i_0 . Enfin, d'après la définition de $\alpha, \beta \geq \alpha + 1$, donc $\beta = \alpha + 1$. On a donc $\operatorname{in} g_{i_0} = \lambda_{i_0} X_n^{\alpha+1}$, $\lambda_{i_0} \neq 0$, ce qui signifie précisément que $\deg g_{i_0} = \alpha + 1$.

Enfin d'après I.4.2, $I \cap k[X_n] = (g_{i_0})k[X_n]$. Si $\xi = (\xi_1,\ldots,\xi_n) \in \overline{k}^n$ est une racine du système $(f_1,\ldots,f_t)$, ξ est une racine de tout $f \in I$ et en particulier de g_{i_0} . Si donc $\alpha_1,\ldots,\alpha_\lambda$, $(\lambda \geq 1)$ sont les racines dans $\overline{k}$ de g_{i_0} , ξ_n coïncide avec l'une de ces racines. Nous allons voir que $\forall i = 1\cdots\lambda$ le système possède au moins une solution de la forme $(\xi_1,\ldots,\xi_{n-1},\alpha_i)$. Pour fixer les idées, considérons α_1 . Soit $k_1 = k(\alpha_1,\ldots,\alpha_\lambda)$ le corps des racines de g_{i_0} et soit $\overline{I}_1$ l'idéal de $k_1[X_1,\ldots,X_n]$ engendré par I . D'après I.2.5 et I.4.2, on a :

$$\overline{I}_1 \cap k_1[X_n] = (g_{i_0})k_1[X_n].$$

Soit maintenant $\phi_1 : k_1[X_1,\ldots,X_n] \to k_1[X_1,\ldots,X_{n-1}]$ le morphisme de k_1-algèbres tel que $\phi_1(X_i) = X_i$, $i = 1\cdots n-1$, $\phi_1(X_n) = \alpha_1$ et soit $I_1 = \phi_1(\overline{I}_1)$. (C'est l'idéal engendré par $(\ldots, f_i(X_1,\ldots,X_{n-1},\alpha_1),\ldots)$. On a :

$$1 \leq \operatorname{rg}_{k_1} k_1[X_1,\ldots,X_{n-1}]/I_1 < \infty.$$

En effet, si ce rang était nul, il existerait $h \in \overline{I}_1$ et $l \in k_1[X_1,\ldots,X_n]$ tel que :

$$1 = h + l(X_n - \alpha_1).$$

Soit $g_{i_0} = \lambda_{i_0}(X_n - \alpha_1)^{m_1}\cdots(X_n - \alpha_\lambda)^{m_\lambda}$ la décomposition de g_{i_0} en facteurs du premier degré dans $k_1[X_n]$ et soit $G_{i_0} = g_{i_0}/X_n - \alpha_1$. On a $G_{i_0} = hG_{i_0} + lg_{i_0} \in \overline{I}_1 \cap k_1[X_n] = (g_{i_0})k_1[X_n]$. C'est impossible.

D'autre part,

$$\operatorname{rg}_k k[X_1,\ldots,X_n]/I = \operatorname{rg}_{k_1} k_1[X_1,\ldots,X_n]/\overline{I}_1 \geq \operatorname{rg}_{k_1} k_1[X_1,\ldots,X_{n-1}]/I_1.$$

En effet, ϕ_1 induit une surjection des espaces vectoriels correspondants. I_1 satisfait donc les mêmes hypothèses que I . Connaissant un système de générateurs de cet idéal, l'algorithme I.3.8 nous permet de déterminer une base standard de cardinal minimal de cet idéal et $g^1 \in k_1[X_{n-1}] \neq 0$ tel que :

$$I_1 \cap k_1[X_{n-1}] = (g^1)k_1[X_{n-1}].$$

de sorte que si $(\xi_1,\ldots,\xi_{n-1}) \in \overline{k}^{n-1}$ vérifie $f(\xi_1,\ldots,\xi_{n-1}) = 0$, $\forall f \in I_1$, $g^1(\xi_{n-1}) = 0$ et ξ_{n-1} coïncide avec une racine α^2 de g^1 . On détermine ainsi successivement des corps k_j , des idéaux $I_j \subset k_j[X_1,\ldots,X_{n-j}]$, des polynômes $g^j \in k_j[X_{n-j}] \neq 0$, des racines $\alpha^{j+1} \in k_{j+1}$ de g^j , $j = 1\cdots n-1$, tels que :

1) k_{j+1} soit le corps des racines de g^j .

2) I_j est l'idéal engendré par $f(X_1,\ldots,X_{n-j},\alpha^j)$, $f \in I_{j-1}$ dans $k_j[X_1,\ldots,X_{n-j}]$.

3) $1 \leq \operatorname{rg}_{k_j} k_j[X_1,\ldots,X_{n-j}]/I_j < \infty$.

4) $I_j \cap k_j[X_{n-j}] = (g^j)k_j[X_{n-j}]$.

De sorte que :

1) Si $(\xi_1,\ldots,\xi_{n-j}) \in \overline{k}^{n-j}$ vérifie $f(\xi_1,\ldots,\xi_{n-j}) = 0$, $\forall f \in I_j$, $g^j(\xi_{n-j}) = 0$.

2) $\{(\xi_1,\ldots,\xi_{n-j}) \in \overline{k}^{n-j}$, $f(\xi_1,\ldots,\xi_{n-j}) = 0$, $\forall f \in I_j\} = \{(\xi_1,\ldots,\xi_{n-j}) \in \overline{k}^{n-j}$, $f(\xi_1,\ldots,\xi_{n-j},\alpha^j) = 0$, $\forall f \in I_{j-1}\}$. Finalement, $(\alpha^n,\ldots,\alpha^2,\alpha_1)$ est une racine de tout $f \in I$ et toute racine du système s'obtient par ce procédé.

1.4. PROPOSITION. — *Si $1 \leq \operatorname{rg} k[X_1,\ldots,X_n]/I < \infty$, le système $(f_1,\ldots,f_t)$ possède un nombre fini s de solutions (sur $\overline{k}$) et*

$$1 \leq s \leq \operatorname{rg}_k k[X_1,\ldots,X_n]/I = \sharp \mathbb{N}^n - \exp I$$

(Remarquer qu'ici, tout ordre vérifiant I.1.1 convient pour calculer ce rang.)

Démonstration. — 1.3 entraîne que $1 \leq s < \infty$. Soit $\alpha_j = (\alpha_{j1}, \ldots, \alpha_{jn}) \in \overline{k}^n$, $j = 1 \cdots s$ les solutions. Soit $\overline{\theta} : \overline{k}[X_1, \ldots, X_n] \to \overline{k}^s$ l'application telle que $\overline{\theta}(f) = (f(\alpha_1), \ldots, f(\alpha_s))$. Elle se factorise au travers $\overline{k}[X_1, \ldots, X_n]/\overline{I}$. Il suffit donc de prouver que $\overline{\theta}$ est surjective. La démonstration se fait par récurrence sur s . Si $s = 1$, c'est évident. Supposons l'assertion vraie pour $s \leq p - 1$. Soit $(\lambda_1, \ldots, \lambda_p) \in \overline{k}^p$; $\exists f \in \overline{k}[X_1, \ldots, X_n]$ tel que $f(\alpha_1) = \lambda_1, \ldots, f(\alpha_{p-1}) = \lambda_{p-1}$. Puisque

$$\begin{array}{llll} \alpha_p \neq \alpha_1 & , \exists i_1 & , 1 \leq i_1 \leq n & , \alpha_{pi_1} \neq \alpha_{1i_1} \\ \vdots & & & \\ \alpha_p \neq \alpha_{p-1} & , \exists i_{p-1} & , 1 \leq i_{p-1} \leq n & , \alpha_{pi_{p-1}} \neq \alpha_{p-1\, i_{p-1}}. \end{array}$$

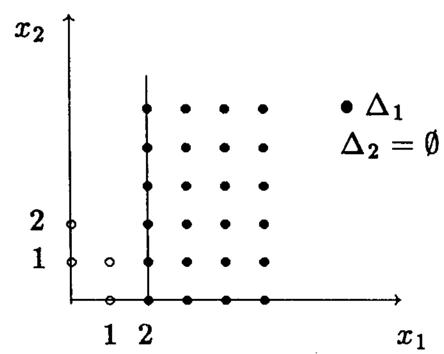
Soit $u(X_1, \ldots, X_n) = (X_{i_1} - \alpha_{1i_1}) \cdots (X_{i_{p-1}} - \alpha_{p-1\, i_{p-1}})$. Il existe $c \in \overline{k}$ tel que $\overline{\theta}(f + cu) = (\lambda_1, \ldots, \lambda_p)$. Soit i , $1 \leq i \leq p - 1$,

$$\begin{aligned} f + cu(\alpha_i) &= \lambda_i + c(\alpha_{ii_1} - \alpha_{1i_1}) \cdots (\alpha_{ii_{p-1}} - \alpha_{p-1\, i_{p-1}}) = \lambda_i \\ f + cu(\alpha_p) &= f(\alpha_p) + c(\alpha_{pi_1} - \alpha_{1i_1}) \cdots (\alpha_{pi_{p-1}} - \alpha_{p-1\, i_{p-1}}) = f(\alpha_p) + c\mu, \mu \neq 0. \end{aligned}$$

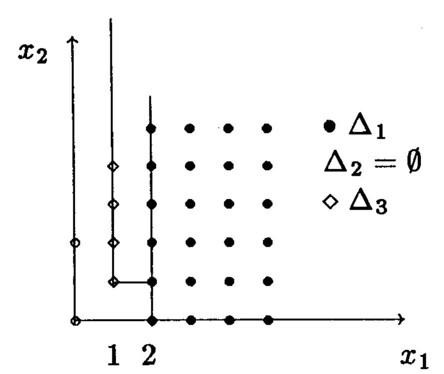
Il existe donc $c \in \overline{k}$ tel que $f(\alpha_p) + c\mu = \lambda_p$.

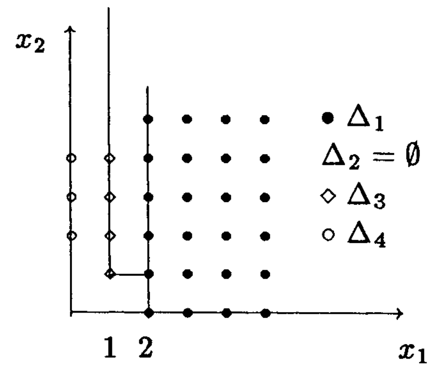
1.5. Exemple . —

$f_1 = X_1^2 + X_1X_2 + 2X_1 + X_2 - 1$
$f_2 = X_1^2 - X_2^2 + 3X_1 + 2X_2 - 1$
in $f_1 = X_1^2$, in $f_2 = X_1^2$
$f_1 S f_2 = f_1 - f_2 = X_1X_2 - X_1 + X_2^2 - X_2$
$f_1 S f_2 R\{f_1, f_2\} = X_1X_2 - X_1 + X_2^2 - X_2 = f_3$
in $f_3 = X_1X_2$



$f_1 S f_2 R\{f_1, f_2, f_3\} = 0$
$f_1 S f_3 = X_2 f_1 - X_1 f_3 = X_1^2 + 3X_1X_2 + X_2^2 - X_2$
$f_1 S f_3 = f_1 + 2f_3 - X_2^2 + 1$
$f_1 S f_3 R\{f_1, f_2, f_3\} = -X_2^2 + 1 = f_4$
in $f_4 = -X_2^2$





$f_1 S f_2 R\{f_1, f_2, f_3, f_4\} = 0$
$f_1 S f_3 R\{f_1, f_2, f_3, f_4\} = 0$
$f_1 S f_4 = -X_2^2 f_1 - X_1^2 f_4 =$
$-f_1 - (X_2^2 + 3X_2 + 2) f_3 - (X_2^2 + X_2 + 1) f_4$
$f_1 S f_4 R\{f_1, f_2, f_3, f_4\} = 0$
$f_2 S f_3 = -X_2 f_1 - X_1 f_3 = f_1 + (X_2 - 2) f_3 - f_4$
$f_2 S f_3 R\{f_1, f_2, f_3, f_4\} = 0$
$f_2 S f_4 = -X_2^2 f_2 - X_1^2 f_4 =$
$-f_1 + (3X_2 + 2) f_3 + (X_2^2 + X_2 + 1) f_4$
$f_2 S f_4 R\{f_1, f_2, f_3, f_4\} = 0$
$f_3 S f_4 = -X_2 f_3 - X_1 f_4 = f_3 + X_2 f_4$
$f_3 S f_4 R\{f_1, f_2, f_3, f_4\} = 0$
(f_1, f_3, f_4) est donc une base standard minimale de I .

$$I \cap k[X_2] = (-X_2^2 + 1) k[X_2].$$

Les racines de $-X_2^2 + 1$ sont 1 et -1 .

Le système possède des solutions de la forme $(\xi, 1)$ et $(\xi, -1)$.

Pour celles du 1er type,

$$I_1 = \big(f_1(X_1, 1), f_2(X_1, 1)\big) k[X_1] = (X_1^2 + 3X_1) k[X_1]$$

$X_1^2 + 3X_1$ possède 0 et -3 comme racines.

Pour celles du 2ème type,

$$\begin{aligned} I_1 &= \big(f_1(X_1, -1), f_2(X_1, -1)\big) k[X_1] \\ &= \big((X_1^2 + X_1 - 2), (X_1^2 + 3X_1 - 4)\big) k[X_1] = (X_1 - 1) k[X_1] \end{aligned}$$

$X_1 - 1$ possède 1 comme racine.

Les racines du système sont donc $(0,1)$, $(-3,1)$ et $(1,-1)$.

$$\mathbf{N}^2 - \exp I = \big((0,0), (0,1), (1,0)\big) \text{ et } \sharp \mathbf{N}^2 - \exp I = 3$$

2. Ensembles et variétés algébriques dans l'espace affine

Soit k un corps, $\overline{k}$ une clôture algébrique de k .

2.1. DÉFINITION . — *L'espace affine à n dimensions sur $\overline{k}$ (noté $\mathbf{A}^n_{\overline{k}}$ ou $\mathbf{A}^n$ quand aucune confusion n'est possible) est ensemblistement $\overline{k}^n$.*

2.1.1. — Si $f \in k[X_1,\ldots,X_n]$, on note $V(f) = \{x \in \overline{k}^n \ , \ f(x) = 0\}$.

2.1.2. — Si $T \subset k[X_1,\ldots,X_n]$, on note $V(T) = \{x \in \overline{k}^n \ , \ f(x) = 0 \ , \forall f \in T\}$. Si I (resp. $\overline{I}$) est l'idéal engendré par T dans $k[X_1,\ldots,X_n]$, (resp. $\overline{k}[X_1,\ldots,X_n]$), on a évidemment $V(T) = V(I) = V(\overline{I})$.

Puisque $k[X_1,\ldots,X_n]$ est noethérien (I.2.3.3), $\forall T \subset k[X_1,\ldots,X_n]$, $\exists f_1,\ldots,f_s \in k[X_1,\ldots,X_n]$ tel que $V(T) = V(f_1) \cap \cdots \cap V(f_s)$. $V(T)$ est l'ensemble des solutions du système $(f_1,\ldots,f_s)$.

2.2. DÉFINITION . — *$Y \subset \mathbf{A}^n_{\overline{k}}$ est appelé k-sous ensemble algébrique de $\mathbf{A}^n_{\overline{k}}$ si et seulement si $\exists T \subset k[X_1,\ldots,X_n]$ tel que $Y = V(T)$.*

2.3. LEMME . — *Si Y_1 et $Y_2 \subset \mathbf{A}^n_{\overline{k}}$ sont 2 k-sous ensembles algébriques de $\mathbf{A}^n_{\overline{k}}$, il en est de même pour $Y_1 \cup Y_2$.*

Si $(Y_\alpha)_{\alpha \in A}$ est une famille de k-sous ensembles algébriques de $\mathbf{A}^n_{\overline{k}}$, il en est de même pour $\cap_{\alpha \in A} Y_\alpha$.

$\emptyset$ et $\mathbf{A}^n_{\overline{k}}$ sont des k-sous ensembles algébriques de $\mathbf{A}^n_{\overline{k}}$.

Démonstration. — Soit I_i , $i = 1,2$, un idéal de $k[X_1,\ldots,X_n]$ tel que $Y_i = V(I_i)$ et soit $I_1.I_2$ l'idéal de $k[X_1,\ldots,X_n]$ engendré par $f_1.f_2$ où $f_i \in I_i$. On a $Y_1 \cup Y_2 = V(I_1.I_2)$. En effet, si $x \in Y_1$, $\forall f \in I_1$, $f(x) = 0$, donc $\forall f \in I_1.I_2$, $f(x) = 0$ et $Y_1 \subset V(I_1.I_2)$.

Réciproquement, si $x \in V(I_1.I_2)$ et si $x \notin Y_1$, $\exists f_1 \in I_1$, $f_1(x) \neq 0$. $\forall f_2 \in I_2$, $f_1 f_2(x) = f_1(x) f_2(x) = 0$; donc $f_2(x) = 0$ et $x \in Y_2$ et $V(I_1.I_2) \subset Y_1 \cup Y_2$.

Si $Y_\alpha = V(I_\alpha)$, I_α idéal de $k[X_1,\ldots,X_n]$, $\cap_{\alpha \in A} Y_\alpha = V(\sum_{\alpha \in A} I_\alpha)$ où $\sum I_\alpha$ est l'idéal de $k[X_1,\ldots,X_n]$ engendré par $\{f \ , \ f \in I_\alpha\}$.

$\emptyset = V(1)$, $\mathbf{A}^n_{\overline{k}} = V(0)$.

2.4. DÉFINITION. — *La topologie de $\mathbf{A}^n_{\overline{k}}$ dont les fermés sont les k- (resp. $\overline{k}$) sous-ensembles algébriques de $\mathbf{A}^n_{\overline{k}}$ est appelée la k-topologie de Zariski (resp. la topologie de Zariski) de $\mathbf{A}^n_{\overline{k}}$.*

2.4.1. EXEMPLE. — Les fermés pour la topologie de Zariski de $\mathbf{A}^1_{\bar{k}}$ sont les ensembles finis de points, $\emptyset$ et $\mathbf{A}^1_{\bar{k}}$.

2.5. DÉFINITION. — *Un sous-ensemble Y non vide d'un espace topologique X est dit **irréductible** si $\forall Y_1, Y_2$ fermés dans Y, $Y_2 \neq Y$ et $Y = Y_1 \cup Y_2$ impliquent $Y = Y_1$.*

2.5.1. EXEMPLE. — $\mathbf{A}^1_{\bar{k}}$ muni de la k-topologie de Zariski (resp. de la topologie de Zariski) est irréductible.

2.5.2. REMARQUE. — Tout ouvert $\neq \emptyset$ dans un espace topologique irréductible est dense. Soit $\Omega \neq \emptyset$ et soit $Y_1 = X - \Omega$ et $Y_2 = \overline{\Omega}$, $Y_1 \neq X$ et $X = Y_1 \cup Y_2$. Donc $Y_2 = \overline{\Omega} = X$.

L'intersection de 2 ouverts non vides d'un espace topologique irréductible est un ouvert non vide.

2.6. DÉFINITION. — *$Y \subset \mathbf{A}^n_{\bar{k}}$ est appelé k-variété algébrique affine (resp. variété algébrique affine) si c'est un fermé irréductible de $\mathbf{A}^n_{\bar{k}}$ pour la k-topologie de Zariski (resp. pour la topologie de Zariski).*

2.6.1. REMARQUE. — Une k-variété algébrique affine n'est pas nécessairement une variété algébrique affine. Par exemple dans $\mathbf{A}^1_{\mathbf{C}}$, $\{i, -i\}$ est un fermé $\mathbf{R}$-irréductible mais pas $\mathbf{C}$-irréductible.

2.7. DÉFINITION. — *Si Y est un sous-ensemble de $\mathbf{A}^n_{\bar{k}}$, on pose*

$$I_k(Y) = \{f \in k[X_1, \dots, X_n], f(x) = 0, \forall x \in Y\}.$$

On écrira parfois $I(Y)$ au lieu de $I_{\bar{k}}(Y)$. $I_k(Y)$ est un idéal de $k[X_1, \dots, X_n]$.

2.8. LEMME. —

i) $I_1 \subset I_2 \Rightarrow V(I_1) \supset V(I_2)$;

ii) Si Y_1 et Y_2 sont des sous-ensembles de $\mathbf{A}^n_{\bar{k}}$,

$$Y_1 \subset Y_2 \Rightarrow I_k(Y_1) \supset I_k(Y_2).$$

iii) Si I est un idéal de $k[X_1, \dots, X_n]$, $\sqrt{I} \subset I_k(V(I))$;

iv) Pour tout sous-ensemble $Y \subset \mathbf{A}^n_{\bar{k}}$, $V(I_k(Y))$ est l'adhérence de Y pour la k-topologie de Zariski.

Démonstration. — *i), ii), iii)* sont clairs.

D'autre part, $Y \subset V(I_k(Y)) \Rightarrow \overline{Y} \subset V(I_k(Y))$. Soit maintenant Z un k-fermé contenant Y. On va montrer que $Z \supset V(I_k(Y))$. En effet $Z = V(I)$ où I est un idéal de $k[X_1, \dots, X_n]$. Puisque $V(I) \supset Y$, $I_k(V(I)) \subset I_k(Y)$. Or $I \subset I_k(V(I))$. Donc $I \subset I_k(Y)$ et $V(I) = Z \supset V(I_k(Y))$.

2.9. PROPOSITION. — *Y un k-sous ensemble algébrique de $\mathbf{A}^n_k$ est une k-variété algébrique affine si et seulement si $I_k(Y)$ est un idéal premier de $k[X_1,\dots,X_n]$.*

Démonstration. — Supposons Y fermé irréductible pour la k-topologie de Zariski de $\mathbf{A}^n_k$ et soit f_i , $i = 1,2$, $f_i \in k[X_1,\dots,X_n]$ tel que $f_1 f_2 \in I_k(Y)$ et $f_1 \notin I_k(Y)$. Soit $W_i = V(f_i)$, $i = 1.2$. Ce sont des k-fermés et $W_1 \cup W_2 = V(f_1 f_2) \supset V(I_k(Y)) = Y$. On a donc $Y = (Y \cap W_1) \cup (Y \cap W_2)$. Or $W_1 \cap Y \neq Y$. En effet, $f_1 \notin I_k(Y)$ et il existe $x \in Y$ tel que $f_1(x) \neq 0$. Y étant k-irréductible et $Y \cap W_i$ étant k-fermés, $Y = Y \cap W_2$. Alors $Y \subset W_2 = V(f_2)$ et $f_2 \in I_k(Y)$.

Réciproquement, supposons $I_k(Y)$ premier et soit Y_1 , Y_2 des k-fermés tels que $Y \neq Y_1$ et $Y = Y_1 \cup Y_2$. Alors $I_k(Y) \supset I_k(Y_1) \cdot I_k(Y_2)$. Puisque $Y \supset Y_1$, $Y \neq Y_1$, $I_k(Y) \subset I_k(Y_1)$ et $I_k(Y) \neq I_k(Y_1)$ (sinon $Y = V(I_k(Y)) = Y_1 = V(I_k(Y_1))$. Il existe alors $f_1 \in I_k(Y_1)$, $f_1 \notin I_k(Y)$. $\forall f_2 \in I_k(Y_2)$, $f_1 f_2 \in I_k(Y)$. $I_k(Y)$ étant premier, $f_2 \in I_k(Y)$. Ainsi $I_k(Y_2) \subset I_k(Y)$ et $V(I_k(Y_2)) = Y_2 \supset V((I_k(Y)) = Y$. Donc $Y_2 = Y$.

2.10. DÉFINITION. — *Un espace topologique X est dit noethérien si pour toute suite décroissante de fermés $Y_1 \supset Y_2 \supset \cdots \supset Y_r \supset Y_{r+1} \supset \cdots$, il existe r tel que $Y_r = \cdots = Y_{r+k} = \cdots$, $\forall k \geq 0$.*

2.11. EXEMPLE . — $\mathbf{A}^n_k$ muni de la k-topologie de Zariski est un espace topologique noethérien. En effet, si $Y_1 \supset Y_2 \supset \cdots \supset Y_r \cdots$, $I_k(Y_1) \subset \cdots \subset I_k(Y_r) \subset I_k(Y_{r+1}) \cdots$. $I = \cup_l I_k(Y_l)$ est un idéal de $k[X_1,\dots,X_n]$. Il est donc engendré par un nombre fini d'éléments $f_1,\dots,f_s$ (I.2.3.3). Soit r tel que $f_i \in I_k(Y_r)$, $i = 1 \cdots s$, $I = I_k(Y_r) = \cdots = I_k(Y_l) = \cdots$, $\forall l \geq r$.

2.12. THÉORÈME. — *Soit X un espace topologique noethérien et Y un fermé de X non vide. Il existe $Y_1,\dots,Y_r$ des fermés irréductibles tels que $Y = Y_1 \cup \cdots \cup Y_r$. Cette décomposition est unique (à l'ordre près des Y_i) si $\forall i = 1 \cdots r$, Y_i n'est pas contenu dans $\cup_{j \neq i} Y_j$. On dit que la décomposition est irrédondante.*

Démonstration. — Supposons qu'il existe un fermé Y qui ne possède pas une telle décomposition. Y est nécessairement réductible. On peut donc écrire $Y = Y_1 \cup Y_2$ où Y_i sont des fermés de X différents de Y . Y_1 et Y_2 ne peuvent tous les deux s'exprimer comme union finie de fermés irréductibles. Si l'assertion d'existence était fausse pour Y , nous pourrions donc construire $Y' \subset Y$, $Y' \neq \emptyset$, $Y' \neq Y$ un fermé pour lequel l'assertion d'existence serait également fausse. On obtiendrait ainsi une suite de fermés strictement décroissante. C'est impossible.

Supposons maintenant que $Y = Y_1 \cup \cdots \cup Y_r = Y'_1 \cup \cdots Y'_{r'}$ soient 2 décompositions irrédondantes en fermés irréductibles. Y_i étant irréductible, puisque $Y_i = (\cup_j Y'_j) \cap Y_i = \cup_j Y'_j \cap Y_i$, il existe j tel que $Y'_j \cap Y_i = Y_i$ et $Y_i \subset Y'_j$. On définit donc ainsi une application $\tau : \{1 \cdots r\} \to \{1 \cdots r'\}$ telle que $Y_i \subset Y'_{\tau(i)}$. Ainsi $Y \subset \cup_{i=1 \cdots r} Y'_{\tau(i)}$ et si $j' \notin \operatorname{Im} \tau$, $Y'_{j'} \subset \cup_{h' \neq j'} Y'_{h'}$. Cette décomposition étant irrédondante, τ est donc surjective et $r' \leq r$. Symétriquement $r \leq r'$ et τ est une permutation de $1 \cdots r$. De la même façon,il existe aussi τ' une permutation de $1 \cdots r$ telle que $Y_j' \subset Y_{\tau'(j)}$. Ainsi, $Y_i \subset Y_{\tau' \circ \tau(i)}$. S'il existe i , tel que $\tau' \circ \tau(i) \neq i$, $Y_i \subset \cup_{j \neq i} Y_j$. C'est impossible et $\tau' \circ \tau = \mathrm{Id}$. Finalement, $Y_i \subset Y'_{\tau(i)} \subset Y_i$ et $Y_i = Y'_{\tau(i)}$.

2.12.1. REMARQUE . — Pour vérifier que la décomposition est irrédondante, il faut et il suffit de vérifier que $Y_i \not\subset Y_j$ si $i \neq j$, $i, j = 1 \cdots r$. En effet, si $Y = Y_1 \cup \cdots \cup Y_r$ était rédondante, il existerait i tel que $Y_i \subset \cup_{j \neq i} Y_j$. Or $Y_i = \cup_{j \neq i} Y_i \cap Y_j$. Y_i étant irréductible, il existe $j \neq i$ tel que $Y_i \cap Y_j = Y_i$ et $Y_i \subset Y_j$.

2.13. DÉFINITION. — *Les Y_i irréductibles apparaissant dans une décomposition irrédondante $Y = Y_1 \cup \cdots \cup Y_r$ d'un fermé Y sont appelés les composantes irréductibles de Y .*

2.13.1. DÉFINITION. — *Si Y est un k-(resp. $\overline{k}$) sous-ensemble algébrique de $\mathbf{A}^n_{\overline{k}}$, $\neq \emptyset$, ses composantes irréductibles pour la k-topologie de Zariski (resp. la topologie de Zariski) de $\mathbf{A}^n_{\overline{k}}$ sont appelées ses k-composantes irréductibles (resp. ses composantes irréductibles géométriques).*

2.14. DÉFINITION. — *Si Y est une k-variété algébrique affine et si K est le corps des fractions de $k[X_1, \ldots, X_n]/I_k(Y)$, on appelle k-dimension de Y le degré de transcendance de K sur k .*

2.14.1. DÉFINITION. — *Si Y est un k-sous ensemble algébrique de $\mathbf{A}^n_{\overline{k}}$, $\neq \emptyset$ et si $Y = Y_1 \cup \cdots \cup Y_r$ est sa décomposition en k-composantes irréductibles, la k-dimension de Y est le maximum des k-dimensions des Y_i , $i = 1 \cdots r$.*

La $\overline{k}$-dimension d'un $\overline{k}$-sous ensemble algébrique Y de $\mathbf{A}^n_{\overline{k}}$ est aussi appelée sa dimension géométrique .

2.14.2. REMARQUE . — Nous montrerons plus loin que la k- dimension d'un k-sous ensemble algébrique Y est un entier fini et qu'elle coïncice avec la dimension géométrique de Y vu comme un $\overline{k}$-sous ensemble algébrique.

3. Des résultats de finitude. Notion d'élément entier

Dans ce paragraphe, B est un anneau *commutatif unitaire noethérien et* A *une* B*-algèbre commutative avec unité de type fini sur* B .

3.1. DÉFINITION. — *Soit* $f \in A$. *On dit que* f *est entier sur* B , *s'il existe* $g_1, \ldots, g_s \in B$ *tel que*

$$f^s + g_1 f^{s-1} + \cdots + g_s = 0 \qquad (*)$$

$(*)$ *est appelée une relation de dépendance intégrale de* f *sur* B .

On dit que A *est entier sur* B *si tout* f *de* A *est entier sur* B .

3.2. LEMME. — *Soit* $f \in A$. *Les conditions suivantes sont équivalentes :*

i) f *est entier sur* B .

ii) $B[f]$ *(la sous* B*-algèbre de* A *engendrée par* f*) est un* B*- module de type fini.*

Démonstration. —

$i) \Rightarrow ii)$: si f est entier sur B et si $f^s + g_1 f^{s-1} + \cdots + g_s = 0$, est une relation de dépendance intégrale, $1, f, \ldots, f^{s-1}$ est un système de générateurs de $B[f]$ en tant que B-module.

$ii) \Rightarrow i)$: soit $e_1, \ldots, e_n \in B[f]$ engendrant $B[f]$ en tant que B-module. Puisque $fe_i \in B[f]$, il existe $\lambda_{ij} \in B$ tels que $fe_i = \sum_j \lambda_{ij} e_j$. On obtient donc dans $B[f]$ n relations

$$\begin{array}{llll} (\lambda_{11} - f)e_1 & + \cdots + \lambda_{1n} e_n & & = 0 \\ \vdots & & & \\ \lambda_{n1} e_1 + \lambda_{n2} e_2 & + \cdots + (\lambda_{nn} - f)e_n & & = 0. \end{array}$$

Soit

$$\delta = \det \begin{vmatrix} \lambda_{11} - f & \lambda_{12} & \cdots \lambda_{1n} \\ \vdots & & \\ \lambda_{n1} & \lambda_{n2} & \cdots \lambda_{nn} - f \end{vmatrix} \ ; \ \delta \in B[f].$$

De ces relations, on déduit que $\delta e_i = 0$, $i = 1 \cdots n$. Il en résulte que $\delta\, B[f] = 0$. En particulier, puisque $1 \in B[f]$, $\delta \cdot 1 = \delta = 0$. C'est la relation de dépendance intégrale cherchée.

3.2.1. PROPOSITION. — *Les conditions suivantes sont équivalentes :*

i) A *est entier sur* B .

ii) A *est un* B*-module de type fini.*

Démonstration. —

$i) \Rightarrow ii)$: A étant une B-algèbre de type fini, soit $f_1, \ldots, f_n$ un système de générateurs de A en tant que B- algèbre. La démonstration est par récurrence sur n . Si $n = 1$, c'est le lemme 3.2. Supposons maintenant que si $A' = B[g_1, \ldots, g_{n-1}]$ et si A' est entier sur B , A' est un B-module de type fini. Alors $A_1 = B[f_1, \ldots, f_{n-1}]$ est un B-module de type fini. Mais $A = A_1[f_n]$, et f_n entier sur B est a fortiori entier sur A_1 . Donc (3.2), A est un A_1-module de type fini. A_1 étant lui-même un B-module de type fini, A l'est aussi.

$ii) \Rightarrow i)$: soit $f \in A$, et soit $A_1 = B[f]$. D'après 3.2, il suffit de montrer que A_1 est un B-module de type fini. Mais A_1 est un sous B-module de A qui est un B-module de type fini et B est noethérien. La conclusion suit alors du lemme suivant :

3.2.2. LEMME. — *Si B est un anneau noethérien et si N est un sous B-module de M , un B-module de type fini, N est un B- module de type fini.*

Démonstration. — Il suffit de montrer le lemme si M est un B-module libre de type fini B^s . En effet, si M est un B-module de type fini, il existe un homomorphisme surjectif $\phi : B^s \to M$. $\phi^{-1}(N)$ est un sous B-module de B^s . Si $e_1, \ldots, e_k$ engendrent $\phi^{-1}(N)$, $\phi(e_1), \ldots, \phi(e_k)$ engendrent N .

La démonstration est maintenant par récurrence sur s . Si $s = 1$, c'est vrai, car tout idéal de B noethérien admet un nombre fini de générateurs.

Soit maintenant $\pi : B^s \to B^{s-1}$, $\pi(\lambda_1, \ldots, \lambda_s) = (\lambda_1, \ldots, \lambda_{s-1})$.

Par hypothèse, $\pi(N)$ est un B-module de type fini. Il existe donc $e_1, \ldots, e_t \in N$ tels que $\pi(e_1), \ldots, \pi(e_t)$ engendrent $\pi(N)$. D'autre part, $\ker \pi$ étant isomorphe à B , $N \cap \ker \pi$ est également engendré par un nombre fini d'éléments $f_1, \ldots, f_{t'} \in N$. Soit maintenant $f \in N$. Il existe $\lambda_1, \ldots, \lambda_t \in B$ tels que $\pi(f) = \lambda_1 \pi(e_1) + \cdots + \lambda_t \pi(e_t)$, $f - \sum \lambda_i e_i \in N \cap \ker \pi$; il existe donc $\mu_1, \ldots, \mu_{t'} \in B$ tels que : $f - \sum \lambda_i e_i = \sum \mu_j f_j$.

3.3. PROPOSITION. — *L'ensemble des éléments de A entiers sur B est une sous-algèbre de A appelée la clôture intégrale de B dans A .*

Démonstration. — Soit f et g des éléments de A entiers sur B . $C = B[f, g]$ est une B-algèbre de type fini. Il suffit donc d'après 3.2.1 de montrer que C est un B-module de type fini puisqu'alors tout élément de C en particulier $f + g$, fg est entier sur B . Or f est entier sur B; $B[f]$ est donc un B-module de type fini. g est entier sur B; a fortiori g est entier sur $B[f]$ et $B[f, g] = C$ est un $B[f]$ module de type fini. C est donc un B-module de type fini.

3.4. PROPOSITION. — *Soit k un corps, $k[X]$ l'anneau de polynômes à une indéterminée sur k . Soit $k(X)$ le corps des fractions de $k[X]$. Si $f \in k(X)$ est entier sur $k[X]$, $f \in k[X]$.*

Démonstration. — Il existe $u, v \in k[X]$ ayant 1 comme PGCD tels que

$f = u/v$. Soit $f^s + g_1 f^{s-1} + \cdots + g_s = 0$, $g_i \in k[X]$, $i = 1 \cdots s$ une relation de dépendance intégrale de f sur $k[X]$. On en déduit

$$u^s + g_1 v u^{s-1} + \cdots + g_s v^s = 0.$$

v divise donc u^s dans $k[X]$. Or il existe $a, b \in k[X]$ tels que

$$1 = au + bv.$$

Puisque $u^{s-1} = au^s + bu^{s-1}v$, v divise donc aussi u^{s-1} . Finalement, v divise 1 . C'est que $v \in k$ et $f \in k[X]$.

4. Les avatars d'un théorème d'existence

Soit k un corps, $\overline{k}$ une clôture algébrique de k et I un idéal de $k[X_1,\dots,X_n]$.

4.1. LEMME. — *Si $I \neq (1)$, I est contenu dans un idéal maximal.*

Démonstration. — Ou bien I est maximal, ou bien non. Alors, il existe un idéal $I_1 \supset I$, $I_1 \neq I$, $I_1 \neq (1)$. Si I_1 lui-même n'était pas maximal, il existerait un idéal $I_2 \supset I_1$, $I_2 \neq I_1$, $I_2 \neq (1)$ etc$\cdots$. Si on ne rencontrait jamais d'idéal maximal, on construirait par ce procédé une suite d'idéaux I_j strictement croissante. Mais $k[X_1,\dots,X_n]$ étant noethérien, $I = \cup_j I_j$ est un idéal engendré par un nombre fini d'éléments $f_1,\dots,f_s$. Soit r tel que $f_i \in I_r$, $i = 1\cdots s$, $I = I_r = I_{r+1} = \cdots$. C'est impossible.

4.2. PROPOSITION. — *Si M est un idéal maximal de $k[X_1,\dots,X_n]$, on a :*

$$1 \leq \operatorname{rg}_k k[X_1,\dots,X_n]/M < +\infty.$$

Démonstration. — Puisque M est maximal, $1 \notin M$ et $k[X_1,\dots,X_n]/M \neq 0$. Son rang sur k est donc ≥ 1 .

Pour montrer que ce rang est fini, nous allons procéder par récurrence sur n .

Si $n = 1$, M est un idéal principal (g) . $g \neq 0$ car (0) n'est pas un idéal maximal de $k[X_1]$. Si d est le degré de g , $1, X_1, \dots, X_1^{d-1}$ est alors une k-base de $k[X_1]/(g)$ (division).

Supposons donc l'assertion vraie pour $n-1$. Soit $J = M \cap k[X_1]$. J est un idéal principal (g) .

Si $g \neq 0$, $\deg g = d \geq 1$. En effet, si $\deg g = 0$, $\exists c \in k$, $c \neq 0$ tel que $c \in J \subset M$ et $1 \in M$, ce qui est impossible. $k[X_1]/(g)$ est donc un espace vectoriel de rang d sur k .

De plus J est un idéal premier. En effet, si $h_1h_2 \in J$ et si $h_1 \notin J$, puisque $h_i \in k[X_1]$, $i = 1,2$, $h_1 \notin M$. Or $h_1h_2 \in M$. M étant maximal, est premier et $h_2 \in M \cap k[X_1] = J$.

C'est en fait un idéal maximal. En effet soit J' un idéal de $k[X_1]$, $J' \supset J$, $J' \neq (1)$. J' est un idéal principal (g') . Puisque $g \in J'$, il existe $f \in k[X_1]$ tel que $g = fg'$. Puisque J est premier, si $g' \notin J$ c'est que $f \in J$. Mais alors, il existe $f' \in k[X_1]$ tel que $f = f'g$. Donc $g = f'gg'$ dans $k[X_1]$. Alors $f'g' = 1$. g' se réduit donc à une constante non nulle de k et $J' = (1)$. Or $J' \neq (1)$. C'est donc que $g' \in J$ et $J' \subset J$. $k[X_1]/J$ est donc un corps k' extension de degré $d \geq 1$ de k .

La surjection canonique $k[X_1,\dots,X_n] \to k[X_1,\dots,X_n]/M$ se factorise en un k-morphisme surjectif :

$$\gamma : k[X_1,\dots,X_n]/(g)\ k[X_1,\dots,X_n] \to k[X_1,\dots,X_n]/M.$$

Or $k[X_1,\dots,X_n]/(g)\ \ k[X_1,\dots,X_n] = k'[X_2,\dots,X_n]$. $k[X_1,\dots,X_n]/M$ est donc k-isomorphe à $k'[X_2,\dots,X_n]/\ker\gamma$. M étant maximal, $k[X_1,\dots,X_n]/M$ est un corps, de même $k'[X_2,\dots,X_n]/\ker\gamma$ et $\ker\gamma$ est un idéal maximal. Appliquant alors l'hypothèse de récurrence à $k'[X_2,\dots,X_n]$ et $\ker\gamma$, il vient $\mathrm{rg}_{k'}\ k[X_1,\dots,X_n]/M < +\infty$. k' étant une extension de degré fini de k , il en résulte que $\mathrm{rg}_k k[X_1,\dots,X_n]/M < +\infty$.

Si maintenant $g = 0$, l'application naturelle $\phi : k[X_1] \to k[X_1,\dots,X_n]/M$ est injective et $k[X_1,\dots,X_n]/M$ étant un corps, elle s'étend à $k(X_1)$ le corps des fractions de $k[X_1]$. Nous avons alors un diagramme commutatif :

$$\begin{array}{ccccc} k & \longrightarrow & k[X_1] & \xrightarrow{\phi} & k[X_1,\dots,X_n]/M \\ & & \downarrow & \nearrow \overline{\phi} & \uparrow \psi \\ & & k(X_1) & \hookrightarrow & k(X_1)[X_2,\dots,X_n] \end{array}$$

où $\psi(\sum u_\alpha X_2^{\alpha_2}\cdots X_n^{\alpha_n}) = \sum \overline{\phi}(u_\alpha)(clX_2 \bmod M)^{\alpha_2}\cdots(clX_n \bmod M)^{\alpha_n}$. Comme ci-dessus, ψ étant surjective, $k[X_1,\dots,X_n]/M \simeq k(X_1)[X_2,\dots,X_n]/\ker\psi$ et $\ker\psi$ est un idéal maximal. Appliquant maintenant l'hypothèse de récurrence à $k(X_1)[X_2,\dots,X_n]$ et $\ker\psi$, nous obtenons que $k[X_1,\dots,X_n]/M$ est un $k(X_1)$-espace vectoriel de rang fini. Il résulte alors de 3.2.1 que pour tout $i = 1\cdots n$, $\overline{X}_i = clX_i \bmod M$ vérifie une relation de dépendance intégrale sur $k(X_1)$.

$$\overline{X}_i^{s_i} + g_1^i\overline{X}_i^{s_i-1} + \cdots + g_{s_i}^i = 0 \quad , \quad g_j^i \in k(X_1)\ ,\ j = 1\cdots s_i.$$

Réduisant à un même dénominateur $v \in k[X_1]$,$v \neq 0$ les g_j^i , $i = 1\cdots n$, $j = 1\cdots s_i$, on détermine $u_j^i \in k[X_1]$, $i = 1\cdots n$, $j = 1\cdots s_i$ tels que

$$\overline{X}_i^{s_i} + \frac{u_1^i}{v}\overline{X}_i^{s_i-1} + \cdots + \frac{u_{s_i}^i}{v} = 0$$

et

$$(v\overline{X}_i)^{s_i} + u_1^i(v\overline{X}_i)^{s_i-1} + \cdots + u_j^i v^{j-1}(v\overline{X}_i)^{s_i-j} + \cdots + u_{s_i}^i v^{s_i-1} = 0$$

$v\overline{X}_i$ est donc entier sur $k[X_1]$, $i = 1\cdots n$.

Or l'ensemble des éléments de $k[X_1,\dots,X_n]/M$ entiers sur $k[X_1]$ est une sous-algèbre de $k[X_1,\dots,X_n]/M$ (3.3). Par suite, $\forall\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbf{N}^n$, $v^{|\alpha|}\overline{X}_1^{\alpha_1}\cdots\overline{X}_n^{\alpha_n}$ est entier sur $k[X_1]$. Plus généralement, v appartenant à $k[X_1]$, si $f \in k[X_1,\dots,X_n]$, $f \neq 0$ est un polynôme de degré d , $v^d f(\overline{X}_1,\dots,\overline{X}_n)$ est entier sur $k[X_1]$. Pour tout $h \in k(X_1)$, $h \neq 0$, il existe donc un entier d dépendant de h tel que $v^d\overline{\phi}(h)$ est entier sur $k[X_1]$. $\overline{\phi}$ étant injective, $v^d h$ est également entier sur $k[X_1]$, donc appartient à $k[X_1]$ (3.4). Il existe donc $u \in k[X_1]$, $h = u/v^d$. On pourrait donc écrire tout $h \in k(X_1)$ avec une puissance de v comme dénominateur. C'est absurde. C'est donc que le cas $g = 0$ est impossible.

4.3. THÉORÈME. — *Soit I un idéal de $k[X_1,\dots,X_n]$, $\neq (1)$. Alors $V(I)$ est non vide.*

Démonstration. — Puisque $I \neq (1)$, I est contenu dans un idéal maximal M (4.1) et $V(M) \subset V(I)$. De 4.2 et 1.4, il résulte que $V(M)$ est un ensemble fini non vide.

4.4. COROLLAIRE. — *Si M est un idéal maximal de $\overline{k}[X_1,\ldots,X_n]$, il existe $x_i \in \overline{k}$, $i = 1\cdots n$ tels que $M = (X_1 - x_1,\ldots,X_n - x_n)$.*

Démonstration. — $V(M)$ étant un ensemble non vide (4.3; 1.4) soit $x \in \overline{k}^n$, $x = (x_1,\ldots,x_n)$, $x \in V(M)$. $\forall f \in M$, $f(x) = 0$. Alors $f \in (X_1 - x_1,\ldots,X_n - x_n)$ (Formule de Taylor). Donc $M \subset (X_1 - x_1,\ldots,X_n - x_n)$ et M étant maximal, on a l'égalité.

4.5. THÉORÈME (Théorème des zéros de Hilbert). — *Soit I un idéal de $k[X_1,\ldots,X_n]$, $\sqrt{I} = I_k(V(I))$.*

Démonstration. — On a déjà vu (2.8.iii) que $\sqrt{I} \subset I_k(V(I))$. Considérons maintenant $f \in I_k(V(I))$. Soit J l'idéal de $k[X_1,\ldots,X_n,T]$ engendré par I et $1 - Tf$. $V(J) = \emptyset$. En effet si $x = (x_1,\ldots,x_n,t) \in \overline{k}^{n+1}$ est dans $V(J)$, $g(x_1,\ldots,x_n) = 0$, $\forall g \in I$. Donc $x_1,\ldots,x_n \in V(I)$, $f(x_1,\ldots,x_n) = 0$ et $1 - tf(x_1,\ldots,x_n) = 1$. De 4.3, on déduit donc que $1 \in J$. Soit $f_1,\ldots,f_s$ un système de générateurs de I . Il existe donc $h_1,\ldots,h_s$, $h \in k[X_1,\ldots,X_n,T]$ tels que

$$1 = h_1 f_1 + \cdots + h_s f_s + h(1 - Tf).$$

Substituant $1/f(X_1,\ldots,X_n)$ à T dans cette relation et chassant les dénominateurs, on détermine un entier ρ tel que $f^\rho \in I$.

4.6. COROLLAIRE. — *Si I est un idéal de $k[X_1,\ldots,X_n] \neq (1)$, il existe $\mathcal{P}_1,\ldots,\mathcal{P}_r$ des idéaux premiers de $k[X_1,\ldots,X_n]$ tels que $\sqrt{I} = \mathcal{P}_1 \cap \cdots \cap \mathcal{P}_r$. Cette décomposition est unique (à l'ordre près des $\mathcal{P}_i$) si $\forall i = 1\cdots r$, $\mathcal{P}_i$ ne contient pas $\cap_{j\neq i}\mathcal{P}_j$. On dit que la décomposition est irrédondante.*

Démonstration. — Soit $V(I) = Y_1 \cup \cdots \cup Y_r$ la décomposition de $V(I)$ en ses k-composantes irréductibles (2.13.1). On a :

$$I_k(V(I)) = I_k(Y_1 \cup \cdots \cup Y_r) = I_k(Y_1) \cap \cdots \cap I_k(Y_r).$$

Or (4.5), $\sqrt{I} = I_k(V(I))$. D'autre part (2.9), $I_k(Y_i)$ est un idéal premier de $k[X_1,\ldots,X_n]$.

Si maintenant $\sqrt{I} = \mathcal{P}_1 \cap \cdots \cap \mathcal{P}_{r'}$ est une décomposition irrédondante de $\sqrt{I}$ en idéaux premiers

$$V(I) = V(\sqrt{I}) = V(\mathcal{P}_1 \cap \cdots \cap \mathcal{P}_{r'}) = V(\mathcal{P}_1) \cup \cdots \cup V(\mathcal{P}_{r'}).$$

En effet, $\mathcal{P}_1 \cdots \mathcal{P}_{r'} \subset \cap_j \mathcal{P}_j$ et $V(\mathcal{P}_1 \cdots \mathcal{P}_{r'}) = \cup V(\mathcal{P}_j) \supset V(\mathcal{P}_1 \cap \cdots \cap \mathcal{P}_{r'})$ (2.3). D'autre part, $\cap_j \mathcal{P}_j \subset \mathcal{P}_i$ et $V(\cap_j \mathcal{P}_j) \supset V(\mathcal{P}_i)$, $\forall i = 1\cdots r'$.

Or (4.5; 2.9), $\mathcal{P}_i = \sqrt{\mathcal{P}_i} = I_k(V(\mathcal{P}_i))$ étant un idéal premier, $V(\mathcal{P}_i)$ est un k-fermé irréductible. La décomposition ainsi obtenue est irrédondante. Sinon il existerait $i \in 1\cdots r'$ tel que

$$V(\mathcal{P}_i) \subset \cup_{j\neq i} V(\mathcal{P}_j) = V(\cap_{j\neq i}\mathcal{P}_j)$$

et

$$I_k(V(\mathcal{P}_i)) = \sqrt{\mathcal{P}}_i = \mathcal{P}_i \supset I_k(V(\cap_{j\neq i}\mathcal{P}_j)) \supset \cap_{j\neq i}\mathcal{P}_j.$$

On a donc $r' = r$ et à permutation près des indices, on peut supposer que $V(\mathcal{P}_i) = Y_i$ et $\mathcal{P}_i = I_k(Y_i)$.

5. La notion de variables commodes

Soit k un corps et I un idéal de $k[X_1,\dots,X_n]$.

5.1. DÉFINITION. — *Soit $f \in k[X_1,\dots,X_n]$, $f \neq 0$. On désigne par* $\operatorname{gr} f$ *la partie homogène de plus haut degré de f . Si $I \neq (0)$, $\operatorname{gr} I$ est l'idéal de $k[X_1,\dots,X_n]$ engendré par $\{\operatorname{gr} f\ ,\ f \in I\ ,\ f \neq 0\}$*

5.1.1. REMARQUE. — Soit $k[X_1,\dots,X_n]_s$ l'ensemble des polynômes homogènes de degré s

$$\operatorname{gr} I = \bigoplus_{s\in\mathbf{N}} \operatorname{gr} I \cap k[X_1,\dots,X_n]_s.$$

Si $F \in \operatorname{gr} I \cap k[X_1,\dots,X_n]_s$, $F \neq 0$, il existe $f \in I$ de degré s tel que $F = \operatorname{gr} f$.

5.2. DÉFINITION. — *Soit I un idéal de $k[X_1,\dots,X_n]$; on dit que les variables $X_1,\dots,X_n$ sont commodes pour I , ou bien si $I = (0)$ ou bien si $I \neq (0)$ et s'il existe un entier d , $0 \leq d < n$ tel que :*

i) l'application canonique $\psi : k[X_{n-d+1},\dots,X_n] \to k[X_1,\dots,X_n]/\operatorname{gr} I$ est injective.

ii) ψ fait de $k[X_1,\dots,X_n]/\operatorname{gr} I$ une $k[X_{n-d+1},\dots,X_n]$-algèbre entière.

(Si $d = 0$, la condition i) signifie que $1 \notin \operatorname{gr} I$, la condition ii) que $k[X_1,\dots,X_n]/\operatorname{gr} I$ est un k-espace vectoriel de rang fini (3.2.1).)

5.3. PROPOSITION. — *Si les variables $X_1,\dots,X_n$ sont commodes pour $I \neq (0)$:*

i) l'application canonique $\phi : k[X_{n-d+1},\dots,X_n] \to k[X_1,\dots,X_n]/I$ est injective.

ii) ϕ fait de $k[X_1,\dots,X_n]/I$ une $k[X_{n-d+1},\dots,X_n]$-algèbre entière.

Démonstration. — Montrons d'abord $i)$. Soit $f \in k[X_{n-d+1},\dots,X_n]$, tel que $\phi(f) = 0$. Alors $f \in I$. Si $f \neq 0$, $\operatorname{gr} f \in \operatorname{gr} I \cap k[X_{n-d+1},\dots,X_n]$. Donc $\psi(\operatorname{gr} f) = 0$ et $\operatorname{gr} f = 0$. Contradiction.

Montrons maintenant $ii)$. D'après 3.2.1, il suffit de montrer que $k[X_1,\dots,X_n]/I$ est un $k[X_{n-d+1},\dots,X_n]$-module de type fini. Or toujours d'après 3.2.1, $k[X_1,\dots,X_n]/\operatorname{gr} I$ est un $k[X_{n-d+1},\dots,X_n]$-module de type fini. Soit $h_1,\dots,h_u \in k[X_1,\dots,X_n]$ tels que $(\dots,H_i = \operatorname{cl} h_i \operatorname{mod} \operatorname{gr} I,\dots)$ soit un système de générateurs de $k[X_1,\dots,X_n]/\operatorname{gr} I$ comme $k[X_{n-d+1},\dots,X_n]$-module.

Posons $h_i = \sum_{\alpha\in\mathbf{N}} h_{i\alpha}$ où $h_{i\alpha} \in k[X_1,\dots,X_n]_\alpha$. $(\dots,H_{i\alpha} = \operatorname{cl} h_{i\alpha} \operatorname{mod} \operatorname{gr} I,\dots)$ est encore un système de générateurs de $k[X_1,\dots,X_n]/\operatorname{gr} I$ en tant que

$k[X_{n-d+1},\ldots,X_n]$-module. En effet, soit $p \in k[X_1,\ldots,X_n]$ un polynôme homogène de degré θ . Il existe $p_i \in k[X_{n-d+1},\ldots,X_n]$, $i = 1\cdots u$, tels que

$$p - \sum_i p_i h_i \in \operatorname{gr} I.$$

D'après 5.1.1, la composante homogène de degré θ appartient aussi à $\operatorname{gr} I$ et si $p_i = \sum_{\beta\in\mathbf{N}} p_{i\beta}$ où $p_{i\beta} \in k[X_{n-d+1},\ldots,X_n]_\beta$, c'est $p - \sum_{i,\alpha+\beta=\theta} p_{i\beta}h_{i\alpha}$.

Montrons maintenant que $(\ldots,\tilde{h}_{i\alpha} = \operatorname{cl} h_{i\alpha} \operatorname{mod} I,\ldots)$ est un système de générateurs de $k[X_1,\ldots,X_n]/I$ comme $k[X_{n-d+1},\ldots,X_n]$-module. Soit $q \in k[X_1,\ldots,X_n]$, $q \neq 0$. Soit θ le degré de q . Il existe $g_{i\alpha} \in k[X_{n-d+1},\ldots,X_n]$ tels que

$$q - \sum g_{i\alpha}h_{i\alpha} \in \operatorname{gr} I.$$

Soit $g_{i\alpha} = \sum_{\beta\in\mathbf{N}} g_{i\alpha\beta}$ où $g_{i\alpha\beta} \in k[X_{n-d+1},\ldots,X_n]_\beta$.

D'après 5.1.1, la composante homogène de degré θ de $q - \sum g_{i\alpha}h_{i\alpha}$ appartient encore à $\operatorname{gr} I$ et c'est $\operatorname{gr} q - \sum_\alpha g_{i\alpha\theta-\alpha}h_{i\alpha}$ et si elle n'est pas nulle, il existe $g \in I$, $g \neq 0$, de degré θ tel que :

$$\operatorname{gr} q - \sum_\alpha g_{i\alpha\theta-\alpha}h_{i\alpha} = \operatorname{gr} g.$$

Dans le premier cas, soit :

$$q_1 = q - \sum_\alpha g_{i\alpha\theta-\alpha}h_{i\alpha}.$$

Dans le deuxième cas, soit :

$$q_1 = q - \sum_\alpha g_{i\alpha\theta-\alpha}h_{i\alpha} - g.$$

Dans les deux cas, $q \operatorname{mod} I = q_1 \operatorname{mod} I + \sum g_{i\alpha\theta-\alpha}\tilde{h}_{i\alpha}$ et si $q_1 \neq 0$, $\deg q_1 < \theta$.

Si $q_1 = 0$, $q \operatorname{mod} I$ est donc combinaison linéaire à coefficients dans $k[X_{n-d+1},\ldots,X_n]$ des $\tilde{h}_{i\alpha}$.

Si $q_1 \neq 0$, on recommence la même construction. On détermine $q_2 \in k[X_1,\ldots,X_n]$ et si $q_2 \neq 0$, $\deg q_2 < \deg q_1$. La suite des degrés d'une suite de polynômes ne pouvant décroître indéfiniment, il existe i tel que $q_i = 0$ et l'assertion est démontrée.

5.3.1. EXEMPLE. — Si les variables $X_1,\ldots,X_n$ satisfont *i*) et *ii*) de 5.3 elles ne sont pas nécessairement commodes. Soit $n = 2$ et $I = X_1 - X_2^2$,

$\phi : k[X_2] \to k[X_1,X_2]/X_1 - X_2^2$ est un isomorphisme.

$\psi : k[X_2] \to k[X_1,X_2]/X_2^2$ n'est pas injective.

5.4. PROPOSITION. — *Soit I un idéal homogène de $k[X_1,\ldots,X_n] \neq (1)$. Soit $H_i = V(X_i)$, $i = 1\cdots n$. Soit d un entier tel que $0 \leq d < n$. Les conditions suivantes sont équivalentes :*

i) $k[X_1,\ldots,X_n]/I$ est une $k[X_{n-d+1},\ldots,X_n]$-algèbre entière.

ii) $V(I) \cap H_{n-d+1} \cap \cdots \cap H_n = 0$.

Démonstration. —

i) $\Rightarrow$ *ii)* : Puisque $I \neq (1)$ et engendré par des polynômes homogènes, $I \subset (X_1, \ldots, X_n)$. Alors $0 \in V(I) \cap H_{n-d+1} \cap \cdots \cap H_n$. Soit maintenant $x = (x_1, \ldots, x_{n-d}, 0, \ldots, 0) \in V(I) \cap H_{n-d+1} \cap \cdots \cap H_n \subset \overline{k}^n$ où $\overline{k}$ est une clôture algébrique de k . Soit j , $1 \leq j \leq n-d$. Ecrivons une relation de dépendance intégrale de $X_j \bmod I = \overline{X}_j$ sur $k[X_{n-d+1}, \ldots, X_n]$. Il existe $g_i \in k[X_{n-d+1}, \ldots, X_n]$, $i = 1 \cdots s$ tels que :

$$X_j^s + g_1 X_j^{s-1} + \cdots + g_s \in I.$$

I étant un idéal homogène, la composante homogène de degré s de cet élément appartient aussi à I . Si G_i est la composante homogène de degré i de g_i , on a donc

$$X_j^s + G_1 X_j^{s-1} + \cdots + G_s \in I.$$

Puisque $x \in V(I)$, $x_j^s + G_1(0, \ldots, 0) x_j^{s-1} + \cdots + G_s(0, \ldots, 0) = 0$. Mais $G_i(0, \ldots, 0) = 0$, $i = 1 \cdots s$ et $x_j = 0$, $j = 1 \cdots n-d$. Alors $x = 0$.

ii) $\Rightarrow$ *i)* : $V(I) \cap H_{n-d+1} \cap \cdots \cap H_n = V(I + (X_{n-d+1}, \ldots, X_n)) = 0$ (2.3).
$I_k(0) = (X_1, \ldots, X_n) = I_k(V(I + (X_{n-d+1}, \ldots, X_n)) = \sqrt{I + (X_{n-d+1}, \ldots, X_n)}$ (4.5). Pour tout j , $1 \leq j \leq n-d$, il existe donc $\rho(j) \in \mathbf{N}$ tel que :

$$X_j^{\rho(j)} \in I + (X_{n-d+1}, \ldots, X_n).$$

Soit $t = (n-d) \max_{j=1 \cdots n-d} \rho(j)$; si $\alpha_1 + \cdots + \alpha_{n-d} \geq t$, $\exists j$, $\alpha_j \geq \rho(j)$ et $X_1^{\alpha_1} \cdots X_{n-d}^{\alpha_{n-d}} \in I + (X_{n-d+1}, \ldots, X_n)$.

Montrons que $(\ldots, \mathrm{cl}\, X_1^{\alpha_1} \cdots X_{n-d}^{\alpha_{n-d}} \bmod I, \ldots)_{\alpha_1 + \cdots + \alpha_{n-d} < t}$ est un système de générateurs de $k[X_1, \ldots, X_n]/I$ comme $k[X_{n-d+1}, \ldots, X_n]$-module.

En effet, soit $X_1^{\alpha_1} \cdots X_{n-d}^{\alpha_{n-d}} X_{n-d+1}^{\alpha_{n-d+1}} \cdots X_n^{\alpha_n}$ un monôme quelconque. Si $\alpha_1 + \cdots + \alpha_{n-d} < t$, sa classe modulo I est bien dans le $k[X_{n-d+1}, \ldots, X_n]$-module engendré par les éléments indiqués.

Si $\alpha_1 + \cdots + \alpha_{n-d} \geq t$, il existe $g \in I$ et $H_i \in k[X_1, \ldots, X_n]$, $i = n-d+1, \ldots, n$ tels que :

$$(*) \qquad X_1^{\alpha_1} \cdots X_{n-d}^{\alpha_{n-d}} = g + \sum_{i=n-d+1, \ldots, n} H_i X_i.$$

Mais I étant un idéal homogène, la composante homogène de degré $\alpha_1 + \cdots + \alpha_{n-d}$ de g appartient aussi à I , de sorte que dans $(*)$, on peut supposer g homogène de degré $\alpha_1 + \cdots + \alpha_{n-d}$ et H_i , $i = n-d+1, \ldots, n$ homogène de degré $\alpha_1 + \cdots + \alpha_{n-d} - 1$ (en les variables $X_1, \ldots, X_n$) . Alors $\mathrm{cl}\, X_1^{\alpha_1} \cdots X_{n-d}^{\alpha_{n-d}} \bmod I = \sum_{i=n-d+1, \ldots, n} X_i \mathrm{cl}\, H_i \bmod I$. Soit $X_1^{\theta_1} \cdots X_n^{\theta_n}$ un monôme figurant dans H_i .

$$\theta_1 + \cdots + \theta_{n-d} \leq \theta_1 + \cdots + \theta_n = \alpha_1 + \cdots + \alpha_{n-d} - 1.$$

On reprend la même construction avec les nouveaux monômes qui apparaissent puis on applique 3.2.1.

5.5. REMARQUE . — Sous les hypothèses de 5.4, $\forall j$, $1 \leq j \leq n-d$, $\exists \alpha_j$, $\alpha_j \in \mathbf{N}$, $\alpha_j \geq 1$, tel que $X_j^{\alpha_j} \in \operatorname{in} I$, pour l'ordre diagonal ainsi que pour l'ordre lexicographique inverse. En effet, soit $X_j^s + G_1 X_j^{s-1} + \cdots + G_s$ l'élément de I construit dans 5.4. $i) \Rightarrow ii)$. Puisque G_i est homogène de degré i en $X_{n-d+1}, \ldots, X_n$, $\operatorname{in}(X_j^s + G_1 X_j^{s-1} + \cdots + G_s) = X_j^s$.

5.6. REMARQUE . — Soit k' une extension de k . Soit I' l'idéal de $k'[X_1, \ldots, X_n]$ engendré par I . Si les variables $X_1, \ldots, X_n$ sont commodes pour I , elles le sont aussi pour I' .

Démonstration. — De I.2.3 et I.2.5, il résulte que $\operatorname{gr} I'$ est l'idéal de $k'[X_1, \ldots, X_n]$ engendré par $\operatorname{gr} I$ (*cf.* 6.1). On a alors

$$k'[X_1, \ldots, X_n]/\operatorname{gr} I' \simeq k[X_1, \ldots, X_n]/\operatorname{gr} I \otimes_k k'.$$

k' étant plat sur k qui est un corps,

$$\psi' : k'[X_{n-d+1}, \ldots, X_n] \to k'[X_1, \ldots, X_n]/\operatorname{gr} I'$$

s'identifie à $\psi \otimes_k k'$ et est injective. D'autre part, d'après 3.2.1, si $k[X_1, \ldots, X_n]/\operatorname{gr} I$ est une $k[X_{n-d+1}, \ldots, X_n]$-algèbre entière, c'est un $k[X_{n-d+1}, \ldots, X_n]$- module de type fini. $k[X_1, \ldots, X_n]/\operatorname{gr} I \otimes_k k'$ est encore un $k[X_1, \ldots, X_n] \otimes_k k'$ -module de type fini donc une $k'[X_1, \ldots, X_n]$-algèbre entière (3.2.1).

5.7. PROPOSITION. — *Soit* $I = (f_1, \ldots, f_s)$ *un idéal de* $k[X_1, \ldots, X_n]$, $\neq (1), \neq (0)$ *et* d *un entier tel que* $0 \leq d < n$ *et que :*

i) $k[X_{n-d+1}, \ldots, X_n] \to k[X_1, \ldots, X_n]/I$ *soit injective.*

ii) $k[X_1, \ldots, X_n]/I$ *soit une* $k[X_{n-d+1}, \ldots, X_n]$*-algèbre entière.*

Soit $x_i \in \overline{k}$ *une clôture algébrique de* k *et soit* $I(x_i)$ *l'idéal de* $\overline{k}[X_1, \ldots, \hat{X}_i, \ldots, X_n]$ *engendré par* $f_j(X_1, \ldots, x_i, \ldots, X_n)$, $j = 1 \cdots s$.

Alors, si $i \geq n-d+1$,

i') $\overline{k}[X_{n-d+1}, \ldots, \hat{X}_i, \ldots, X_n] \to \overline{k}[X_1, \ldots, \hat{X}_i, \ldots, X_n]/I(x_i)$ *est injectif.*

ii') $\overline{k}[X_1, \ldots, \hat{X}_i, \ldots, X_n]/I(x_i)$ *est une* $\overline{k}[X_{n-d+1}, \ldots, \hat{X}_i, \ldots, X_n]$*-algèbre entière.*

Démonstration. — Les mêmes arguments qu'en 5.6 montrent que $i)$ et $ii)$ restent vrais si on remplace k par $\overline{k}$ et I par $\overline{I}$ l'idéal de $k[X_1, \ldots, X_n]$ engendré par $f_1, \ldots, f_s$.

Soit $f \in \overline{k}[X_{n-d+1}, \ldots, \hat{X}_i, \ldots, X_n] \cap I(x_i)$. D'après la formule de Taylor, il existe $g \in \overline{k}[X_1, \ldots, X_n]$ tel que $f - (X_i - x_i) g \in \overline{I}$. Or $\operatorname{cl} g \bmod \overline{I}$ est entier sur $\overline{k}[X_{n-d+1}, \ldots, X_n]$. Il existe donc $a_1, \ldots, a_s \in \overline{k}[X_{n-d+1}, \ldots, X_n]$ tels que

$$g^s + a_1 g^{s-1} + \cdots + a_s \in \overline{I}$$

et

$$f^s + a_1 (X_i - x_i) f^{s-1} + \cdots + a_s (X_i - x_i)^s \in \overline{I} \cap \overline{k}[X_{n-d+1}, \ldots, X_n].$$

On a donc $f^s + a_1(X_i - x_i)f^{s-1} + \cdots + a_s(X_i - x_i)^s = 0$ dans $\overline{k}[X_{n-d+1}, \ldots, X_n]$ et substituant x_i à X_i , il vient $f^s = 0$ et $f = 0$.

ii') est immédiat.

5.8. COROLLAIRE. — *Sous les hypothèses de 5.7, pour tout* $(x_{n-d+1}, \ldots, x_n) \in \overline{k}^d$, $V(I) \cap \bigcap_{i=n-d+1,\ldots,n} V(X_i - x_i)$ *est un ensemble fini non vide.*

Démonstration. — Si $I(x_{n-d+1}, \ldots, x_n)$ est l'idéal de $\overline{k}[X_1, \ldots, X_{n-d}]$ engendré par $f_j(X_1, \ldots, X_{n-d}, x_{n-d+1}, \ldots, x_n)$, $j = 1 \cdots s$, il résulte de 5.7 que $1 \leq \mathrm{rg}_{\overline{k}} \overline{k}[X_1, \ldots, X_{n-d}]/I(x_{n-d+1}, \ldots, x_n) < +\infty$. $V(I(x_{n-d+1}, \ldots, x_n)) \subset \overline{k}^{n-d}$ est donc un ensemble fini non vide et aussi $V(I) \cap \bigcap_{i=n-d+1,\ldots,n} V(X_i - x_i)$.

L'algorithme 1.3 permet donc connaissant des variables commodes pour I de déterminer les solutions.

6. Détermination de variables commodes

Dans ce paragraphe, k *est un corps infini* et I un idéal de $k[X_1,\ldots,X_n]$, dont on s'est donné un système de générateurs. Si $I \neq (1)$, nous allons montrer comment, connaissant ces générateurs, déterminer un changement de variables linéaire –i.e. un isomorphisme de k-algèbres $\tau : k[X_1,\ldots,X_n] \to k[Y_1,\ldots,Y_n]$ tel que $\tau(X_i)$ soit une forme linéaire en les Y_j , $j = 1\cdots n$, $i = 1\cdots n$, tel que les variables $Y_1,\ldots,Y_n$ soient commodes pour $\tau(I)$.

6.1. LEMME. — *Si H est un idéal homogène de $k[X_1,\ldots,X_n] \neq (0)$ et si $f_1,\ldots,f_t$ est une base standard de H pour l'ordre diagonal,* $\operatorname{gr} f_1,\ldots,\operatorname{gr} f_t$ *est une base standard de H à la fois pour l'ordre diagonal et pour l'ordre lexicographique.(I.1.1.2.1)*

En particulier, si $I \neq (0)$ et si $(f_1,\ldots,f_t)$ est une base standard de I pour l'ordre diagonal, $(\operatorname{gr} f_1,\ldots,\operatorname{gr} f_t)$ *est une base standard de* $\operatorname{gr} I$ *pour l'ordre diagonal et pour l'ordre lexicographique.*

Démonstration. — Soit $f \in k[X_1,\ldots,X_n]$, $f \neq 0$. Notons $\exp_{\text{diag}} f$ (resp. $\exp_{\text{lex}} f$) l'exposant privilégié de f pour l'ordre diagonal (resp. l'ordre lexicographique).

Montrons que $\exp_{\text{diag}} H = \exp_{\text{lex}} H$. Soit $h \in H$, $h \neq 0$, $h = h_0 + \cdots + h_d$ où $h_i \in k[X_1,\ldots,X_n]$ est homogène de degré i , $i = 0\cdots d$ et $h_d \neq 0$. Par définition, $\exp_{\text{diag}} h = \exp_{\text{lex}} h_d$. Or $h_d \in H$. Donc $\exp_{\text{diag}} H \subset \exp_{\text{lex}} H$. D'autre part, $\exp_{\text{lex}} h = \max_i \exp_{\text{lex}} h_i$. Il existe donc i_0 , $1 \leq i_0 \leq d$ tel que $\exp_{\text{lex}} h = \exp_{\text{lex}} h_{i_0} = \exp_{\text{diag}} h_{i_0}$. Mais $h_{i_0} \in H$ et $\exp_{\text{lex}} H \subset \exp_{\text{diag}} H$. $f_1,\ldots,f_t$ étant une base standard de H pour l'ordre diagonal,

$$\begin{aligned}\exp_{\text{diag}} H &= \cup_i \exp_{\text{diag}} f_i + \mathbf{N}^n = \cup_i \exp_{\text{diag}} \operatorname{gr} f_i + \mathbf{N}^n \\ &= \cup_i \exp_{\text{lex}} \operatorname{gr} f_i + \mathbf{N}^n = \exp_{\text{lex}} H.\end{aligned}$$

Il reste à voir que si $f_1,\ldots,f_t$ est une base standard de I pour l'ordre diagonal, $\operatorname{gr} f_1,\ldots,\operatorname{gr} f_t$ est une base standard de $\operatorname{gr} I$ pour l'ordre diagonal.

En effet, si $f \in I$,$f \neq 0$, $\exp_{\text{diag}} f = \exp_{\text{diag}} \operatorname{gr} f$. Donc $\exp_{\text{diag}} I \subset \exp_{\text{diag}} \operatorname{gr} I$.

Si maintenant $F \in \operatorname{gr} I$, $F \neq 0$ et si $F = F_0 + \cdots + F_d$ où F_i est homogène de degré i , $i = 0,\ldots,d$ et $F_d \neq 0$, $\exp_{\text{diag}} F = \exp_{\text{diag}} F_d$. Or (5.1.1), $F_d \in \operatorname{gr} I$ et il existe $f \in I$ de degré d tel que $F_d = \operatorname{gr} f$. Donc $\exp_{\text{diag}} F = \exp_{\text{diag}} \operatorname{gr} f = \exp_{\text{diag}} f$ et $\exp_{\text{diag}} \operatorname{gr} I \subset \exp_{\text{diag}} I$.

Or $\exp_{\text{diag}} I = \cup_i \exp_{\text{diag}} f_i + \mathbf{N}^n = \cup_i \exp_{\text{diag}} \operatorname{gr} f_i + \mathbf{N}^n = \exp_{\text{diag}} \operatorname{gr} I$.

6.2. REMARQUE. — L'algorithme de I.3.5 nous permet donc connaissant un système de générateurs de I de déterminer une base standard pour les ordres diagonaux et lexicographiques de $\operatorname{gr} I$ donc en particulier un système de générateurs de $\operatorname{gr} I$.

6.3. ALGORITHME DE DÉTERMINATION DE VARIABLES COMMODES. Si d'abord $I = (0)$, les variables $X_1, \ldots, X_n$ sont commodes pour I . Si $I \neq (0)$, l'algorithme I.3.5 nous permet d'obtenir connaissant un système de générateurs de I , une base standard pour l'ordre diagonal $(f_1, \ldots, f_s)$ de I et de déterminer $\exp_{\text{diag}} I$. Nous savons (I.2.9) que $I = (1)$ si et seulement $\exp_{\text{diag}} I = \mathbf{N}^n$. Supposons qu'il n'en soit pas ainsi. Alors $\operatorname{gr} I = (\operatorname{gr} f_1, \ldots, \operatorname{gr} f_s) \neq (0), \neq (1)$ (6.1, 6.2).

Soit $x_1 = (\lambda_{11}, \ldots, \lambda_{n1}) \in k^n \notin V(\operatorname{gr} I)$. Un tel point existe car k a été supposé infini (nous reviendrons plus loin sur sa détermination) et choisissons $x_i = (\lambda_{1i}, \ldots, \lambda_{ni}) \in k^n$, $i = 2 \cdots n$ tels que la matrice $\Lambda = (\lambda_{ij})$ soit inversible. Par exemple, si $i_0 = \inf i$, $\lambda_{i1} \neq 0$, on peut choisir, $e_1, \ldots, e_n$ désignant la base canonique de k^n , $x_i = e_{i-1}$, $2 \leq i \leq i_0$, $x_i = e_i$, $i_0 + 1 \leq i \leq n$.

Soit $\tau : k[X_1, \ldots, X_n] \to k[X'_1, \ldots, X'_n]$ le morphisme de k-algèbre tel que $\tau(X_i) = L_i(X'_1, \ldots, X'_n) = \sum_j \lambda_{ij} X'_j$. τ est un changement de variables linéaire.

Soit $\pi : \overline{k}^n \to \overline{k}^n$ (où $\overline{k}$ est une clôture algébrique de k) tel que $\pi(x'_1, \ldots, x'_n) = (\ldots, L_i(x'_1, \ldots, x'_n), \ldots)$; π est un isomorphisme et $e'_1, \ldots, e'_n$ étant la base canonique du $\overline{k}^n$ source, $\pi(e'_i) = x_i$. Soit $I' = \tau(I)$. On a $\operatorname{gr} I' = \tau(\operatorname{gr} I)$ et $V(\operatorname{gr} I') = \pi^{-1}(V(\operatorname{gr} I))$. Posant $H'_i = V(X'_i)$, $i = 2 \cdots n$, on a alors :

$$\begin{aligned} V(\operatorname{gr} I') \cap H'_2 \cap \cdots \cap H'_n = V(\operatorname{gr} I') \cap \overline{k} e'_1 &= \pi^{-1}(V(\operatorname{gr} I)) \cap \pi^{-1}(\overline{k} x_1) \\ &= \pi^{-1}(V(\operatorname{gr} I) \cap \overline{k} x_1) = \pi^{-1}(0) = 0. \end{aligned}$$

Puisque $\operatorname{gr} I' \neq (1)$, d'après 5.4, $k[X'_1, \ldots, X'_n]/\operatorname{gr} I'$ est une $k[X'_2, \ldots, X'_n]$-algèbre entière.

Soit maintenant $\psi' : k[X'_2, \ldots, X'_n] \to k[X'_1, \ldots, X'_n]/\operatorname{gr} I'$ l'application canonique. $\ker \psi' = \operatorname{gr} I' \cap k[X'_2, \ldots, X'_n]$. Puisque $\operatorname{gr} I = (\operatorname{gr} f_1, \ldots, \operatorname{gr} f_s)$, $\operatorname{gr} I' = (\tau(\operatorname{gr} f_1), \ldots, \tau(\operatorname{gr} f_s))$. Ordonnons maintenant les monômes de $k[X'_1, \ldots, X'_n]$ au moyen de l'ordre diagonal. L'algorithme I.3.5 nous permet d'obtenir à partir de ce système de générateurs de $\operatorname{gr} I'$ une base standard pour l'ordre diagonal, puis (6.1) une base standard $(G'_1, \ldots, G'_{u'})$ de $\operatorname{gr} I'$ à la fois pour l'ordre diagonal et l'ordre lexicographique, formée de polynômes homogènes.

Soit $J' = \{i\ ,\ i = 1 \cdots u'\ ;\ G'_i \in k[X'_2, \ldots, X'_n]\}$. Si $J' = \emptyset$, d'après I.4.2, $\operatorname{gr} I' \cap k[X'_2, \ldots, X'_n] = 0$ et les variables $X'_1, \ldots, X'_n$ sont commodes pour I' (l'entier d vaut alors $n - 1$). Si $J' \neq \emptyset$, $(\ldots, G'_i, \ldots)_{i \in J'}$ est une base standard pour l'ordre lexicographique (I.4.2) donc un système de générateurs (I.2.3) de $\operatorname{gr} I' \cap k[X'_2, \ldots, X'_n]$ qui est aussi $\neq (1)$.

Soit $x'_2 = (\lambda'_{22}, \ldots, \lambda'_{n2}) \in k^{n-1} \notin V(\operatorname{gr} I' \cap k[X'_2, \ldots, X'_n])$ et choisissons $x'_i = (\lambda'_{2i}, \ldots, \lambda'_{ni}) \in k^{n-1}$, $i = 3 \cdots n$ tels que la matrice $n - 1 \times n - 1$ $\Lambda' = (\lambda'_{ij})$ soit inversible.

Soit $\tau' : k[X'_1,\ldots,X'_n] \to k[X''_1,\ldots,X''_n]$ le morphisme de k- algèbre tel que $\tau'(X'_1) = L'_1(X''_1,\ldots,X''_n) = X''_1$, $\tau'(X'_i) = L'_i(X''_1,\ldots,X''_n) = \sum_{j=2\cdots n} \lambda'_{ij} X''_j$, $i = 2\cdots n$. τ' est un changement de variables linéaire.

Soit $\pi' : \overline{k}^n \to \overline{k}^n$ tel que $\pi'(x''_1,\ldots,x''_n) = (\ldots, L'_i(x''_1,\ldots,x''_n),\ldots)$; π' est un isomorphisme et $e''_1 \ldots e''_n$ désignant la base canonique du $\overline{k}^n$ source $\pi'(e''_1) = e'_1$, $\pi'(e''_i) = x'_i$, $i = 2\cdots n$.

Soit $I'' = \tau'(I')$. On a $\operatorname{gr} I'' = \tau'(\operatorname{gr} I')$ et $V(\operatorname{gr} I'') = \pi'^{-1}(V(\operatorname{gr} I'))$. Posant $H''_i = V(X''_i)$, $i = 3\cdots n$ on a alors

$$\begin{aligned} V(\operatorname{gr} I'') \cap H''_3 \cap \cdots \cap H''_n &= V(\operatorname{gr} I'') \cap (\overline{k}e''_1 \oplus \overline{k}e''_2) \\ &= \pi'^{-1}\big(V(\operatorname{gr} I')\big) \cap \pi'^{-1}(\overline{k}e'_1 \oplus \overline{k}x'_2) \\ &= \pi'^{-1}\big(V(\operatorname{gr} I') \cap (\overline{k}e'_1 \oplus \overline{k}x'_2)\big). \end{aligned}$$

Or $V(\operatorname{gr} I') \cap (\overline{k}e'_1 \oplus \overline{k}x'_2) = (0)$. En effet, puisque $x'_2 \in \bigoplus_{i\geq 2} \overline{k}e'_i$, si $\xi' = (\xi'_1,\ldots,\xi'_n) \in \overline{k}e'_1 \oplus \overline{k}x'_2$, $(0,\xi'_2,\ldots,\xi'_n) \in \overline{k}x'_2$. En particulier, pour tout $f \in \operatorname{gr} I' \cap k[X'_2,\ldots,X'_n]$, $f(\xi'_2,\ldots,\xi'_n) = 0$; $(\xi'_2,\ldots,\xi'_n)$ appartient donc à $V\big(\operatorname{gr} I' \cap k[X'_2,\ldots,X'_n]\big)$. Si $(\xi'_2,\ldots,\xi'_n) \neq 0$, $\operatorname{gr} I'$ étant un idéal homogène, alors $x'_2 \in V(\operatorname{gr} I' \cap k[X'_2,\ldots,X'_n])$ contrairement à l'hypothèse. Donc, $\xi' = \xi'_1 e'_1$. De même, si $\xi'_1 \neq 0$, on déduirait que $e'_1 \in V(\operatorname{gr} I')$ et $\pi(e'_1) = x_1 \in \pi(V(\operatorname{gr} I')) = V(\operatorname{gr} I)$, contrairement à l'hypothèse. Donc $\xi' = 0$.

π' étant un isomorphisme, on a donc $V(\operatorname{gr} I'') \cap H''_3 \cap \cdots \cap H''_n = 0$ et d'après 5.4, $k[X''_1,\ldots,X''_n]/\operatorname{gr} I''$ est une $k[X''_3,\ldots,X''_n]$-algèbre entière. La détermination d'une base standard de $\operatorname{gr} I'' = \big(\tau' \circ \tau(\operatorname{gr} f_1),\ldots,\tau' \circ \tau(\operatorname{gr} f_s)\big)$ à la fois pour l'ordre diagonal et pour l'ordre lexicographique, formée de polynômes homogènes, nous permet de tester si $\operatorname{gr} I'' \cap k[X''_3,\ldots,X''_n] = (0)$ ou $\neq (0)$. Dans le premier cas, les variables $X''_1,\ldots,X''_n$ sont commodes pour I'' (l'entier d vaut alors $n-2$). Dans le second cas, on détermine un nouveau changement de variables, en choisissant un point de k^{n-2} , hors de $V(\operatorname{gr} I'' \cap k[X''_3,\ldots,X''_n]) \cdots$ etc$\cdots$

Si on a été amené à effectuer $n-1$ changements de variables $\tau,\tau',\ldots,\tau^{(n-2)}$ et si avec $I^{(n-1)} = \tau^{(n-2)} \circ \cdots \circ \tau(I)$,

$$\operatorname{gr} I^{(n-1)} \cap k[X_n^{(n-1)}] = (0)$$

les variables $X_1^{(n-1)},\ldots,X_n^{(n-1)}$ sont commodes pour $I^{(n-1)}$ (l'entier d vaut 1).

Si $\operatorname{gr} I^{(n-1)} \cap k[X_n^{(n-1)}] \neq 0$, cet idéal étant homogène, principal, $\neq (1)$ est engendré par une puissance de $X_n^{(n-1)}$. Si $\xi^{(n-1)} = (\xi_1^{(n-1)},\ldots,\xi_n^{(n-1)}) \in V(\operatorname{gr} I^{(n-1)})$, puisque $X_n^{(n-1)} \in \sqrt{\operatorname{gr} I^{(n-1)}}$, $\xi_n^{(n-1)} = 0$.

Mais $k[X_1^{(n-1)},\ldots,X_n^{(n-1)}]/\operatorname{gr} I^{(n-1)}$ est une $k[X_n^{(n-1)}]$-algèbre entière. D'après 5.4, si $H_n^{(n-1)} = V(X_n^{(n-1)})$, $V(\operatorname{gr} I^{(n-1)}) \cap H_n^{(n-1)} = 0$. Finalement, $V(\operatorname{gr} I^{(n-1)}) = 0$. Toujours d'après 5.4 (cas $d=0$), $k[X_1^{(n-1)},\ldots,X_n^{(n-1)}]/\operatorname{gr} I^{(n-1)}$ est un k-espace vectoriel de rang fini et puisque $1 \notin \operatorname{gr} I^{(n-1)}$, les conditions *i)* et *ii)* de 5.2 sont satisfaites avec $d = 0$. Les variables $X_1^{(n-1)},\ldots,X_n^{(n-1)}$ sont commodes pour $I^{(n-1)}$ (l'entier d vaut 0).

6.4. REMARQUE. — Etant donné un idéal homogène H de $k[X_1,\dots,X_n] \neq 0$, dont on connait un système de générateurs $(h_1,\dots,h_s)$ homogènes, il reste à préciser comment on détermine $x \in k^n$, tel que $x \notin V(H)$. Il suffit évidemment qu'il existe i , $1 \leq i \leq s$ tel que $h_i(x) \neq 0$ et il suffit donc de résoudre le même problème pour H principal. Soit h un générateur homogène de H . S'il existe j , tel que $h(0,\dots,1,\dots,0) \neq 0$, $(0,\dots,1,\dots,0)$ convient. (Le changement de variable associé sera alors une simple permutation). En général un petit nombre d'essai conduira à trouver un x convenable.

Si on veut être plus systématique, soit d le degré de h .

$$h = h_0(X_2,\dots,X_n)X_1^k + \cdots + h_k(X_2,\dots,X_n)$$

où h_j est homogène de degré $d-k+j$ en $X_2,\dots,X_n$ et $h_0 \not\equiv 0$.

Si $\deg h_0 = 0$ (i.e. $d=k$), $h(1,0,\dots,0) \neq 0$.

Si $\deg h_0 \neq 0$, il suffit de déterminer $x' \in k^{n-1}$ tel que $h_0(x') \neq 0$, ensuite on choisira $x_1 \in k$ tel que $h_0(x')x_1^k + \cdots + h_k(x') \neq 0$. Ce polynôme de $k[X_1]$ possède au plus k racines. On est donc ramené au même problème mais dans $k[X_2,\dots,X_n]$.

6.5. PROPOSITION. — *Soit I un idéal de $k[X_1,\dots,X_n] \neq (1), \neq (0)$. Soit d un entier tel que $0 \leq d < n$. Si*

i) $k[X_{n-d+1},\dots,X_n] \to k[X_1,\dots,X_n]/I$ est injective.

ii) $k[X_1,\dots,X_n]/I$ est une $k[X_{n-d+1},\dots,X_n]$-algèbre entière,
d est la k-dimension de $V(I)$.

Démonstration. — Soit $V(I) = Y_1 \cup \cdots \cup Y_r$ une décomposition irrédondante de $V(I)$ en k-fermés irréductibles, (2.12) et soit $P_i = I_k(Y_i), i = 1\cdots r$. P_i est premier (2.9) et $\sqrt{I} = P_1 \cap \cdots \cap P_r$ et cette décomposition est irrédondante (4.6). Puisque $I \cap k[X_{n-d+1},\dots,X_n] = (0)$, $\sqrt{I} \cap k[X_{n-d+1},\dots,X_n] = (0)$ (si $f \in k[X_{n-d+1},\dots,X_n] \cap \sqrt{I}$, $\exists \rho$, $f^\rho \in I \cap k[X_{n-d+1},\dots,X_n] = 0$) . D'autre part, $P_i \cap k[X_{n-d+1},\dots,X_n]$, $i = 1\cdots r$,et (0) sont des idéaux premiers de $k[X_{n-d+1},\dots,X_n]$ et

$$(0) = \cap_{i=1\cdots r}(P_i \cap k[X_{n-d+1},\dots,X_n]).$$

De 4.6, on déduit que ou bien $r=1$, ou bien cette décomposition n'est pas irrédondante. Finalement $J = \{i, 1 \leq i \leq r, P_i \cap k[X_{n-d+1},\dots,X_n] = (0)\}$ est non vide. Soit K_i le corps des fractions de $k[X_1,\dots,X_n]/P_i$.

Nous allons d'abord voir que si $i \in J$, $\deg \mathrm{tr} K_i : k = d$. En effet, l'application canonique $k[X_{n-d+1},\dots,X_n] \to k[X_1,\dots,X_n]/P_i$ étant injective, elle s'étend en une injection de $k(X_{n-d+1},\dots,X_n)$ dans K_i . De plus, $k[X_1,\dots,X_n]/I$ étant une $k[X_{n-d+1},\dots,X_n]$-algèbre entière, il en est de même de $k[X_1,\dots,X_n]/P_i$. $(I \subset P_i)$. Soit L_i l'ensemble des éléments de K_i algébriques sur $k(X_{n-d+1},\dots,X_n)$. C'est un sous-corps de K_i qui contient $k[X_1,\dots,X_n]/P_i$ (un élément entier est a fortiori algébrique). C'est donc K_i . K_i est donc une extension algébrique de $k(X_{n-d+1},\dots,X_n)$ et $\deg \mathrm{tr} K_i : k = d$.

Nous allons maintenant voir que si $i \notin J$, $\deg \mathrm{tr} K_i : k < d$. Soit alors $\tau' : k[X_{n-d+1}, \ldots, X_n] \to k[X'_{n-d+1}, \ldots, X'_n]$ un changement de variables linéaire tel que les variables $X'_{n-d+1}, \ldots, X'_n$ soient commodes pour $\tau'(\mathcal{P}_i \cap k[X_{n-d+1}, \ldots, X_n])$. τ' existe d'après 6.3 car $1 \notin \mathcal{P}_i \cap k[X_{n-d+1}, \ldots, X_n]$ sinon, $\mathcal{P}_i \supset \mathcal{P}_j$, $j = 1 \cdots r$ et la décomposition ne serait pas irrédondante.

Il existe donc d' entier tel que $0 \leq d' < d$ tel que :

i) $k[X'_{n-d'+1}, \ldots, X'_n] \to k[X'_{n-d+1}, \ldots, X'_n]/\tau'(\mathcal{P}_i \cap k[X_{n-d+1}, \ldots, X_n])$ soit injective.

ii) $k[X'_{n-d+1}, \ldots, X'_n]/\tau'(\mathcal{P}_i \cap k[X_{n-d+1}, \ldots, X_n])$ soit une $k[X'_{n-d'+1}, \ldots, X'_n]$-algèbre entière (5.3).

Soit $\overline{\tau}' : k[X_1, \ldots, X_n] \to k[X'_1, \ldots, X'_n]$ tel que $\overline{\tau}'(X_i) = X'_i$, $i = 1 \cdots n-d$, $\overline{\tau}'(X_i) = \tau'(X_i)$, $i = n-d+1, \ldots, n$. $\overline{\tau}'$ est un changement de variables linéaire.

$k[X'_{n-d'+1}, \ldots, X'_n] \to k[X'_1, \ldots, X'_n]/\overline{\tau}'(\mathcal{P}_i)$ est injective. En effet, si $f \in k[X'_{n-d'+1}, \ldots, X'_n] \cap \overline{\tau}'(\mathcal{P}_i)$, il existe $g \in \mathcal{P}_i$ tel que $f = \overline{\tau}'(g)$. Or $k[X'_{n-d'+1}, \ldots, X'_n] \subset k[X'_{n-d+1}, \ldots, X'_n]$. $\overline{\tau}'^{-1}|k[X'_{n-d+1}, \ldots, X'_n] = \tau'^{-1}$. Donc $g \in \mathcal{P}_i \cap k[X_{n-d+1}, \ldots, X_n]$ et $f = \tau'(g)$. Finalement, $f \in k[X'_{n-d'+1}, \ldots, X'_n] \cap \tau'(\mathcal{P}_i \cap k[X_{n-d+1}, \ldots, X_n]) = 0$.

$k[X'_1, \ldots, X'_n]/\overline{\tau}'(\mathcal{P}_i)$ est une $k[X'_{n-d'+1}, \ldots, X'_n]$ -algèbre entière. En effet, nous savons déjà que $k[X_1, \ldots, X_n]/\mathcal{P}_i$ est une $k[X_{n-d+1}, \ldots, X_n]$ algèbre entière. Or on a un diagramme commutatif:

$$\begin{array}{ccc} k[X_{n-d+1}, \ldots, X_n] & \longrightarrow & k[X_1, \ldots, X_n]/\mathcal{P}_i \\ \downarrow & \nearrow & \\ k[X_{n-d+1}, \ldots, X_n]/\mathcal{P}_i \cap k[X_{n-d+1}, \ldots, X_n] & & \end{array}$$

$k[X_1, \ldots, X_n]/\mathcal{P}_i$ est donc une $k[X_{n-d+1}, \ldots, X_n]/\mathcal{P}_i \cap k[X_{n-d+1}, \ldots, X_n]$-algèbre entière. D'après 3.2.1, c'est également un module de type fini. $k[X'_1, \ldots, X'_n]/\overline{\tau}'(\mathcal{P}_i)$ est donc aussi un $k[X'_{n-d+1}, \ldots, X'_n]/\tau'(\mathcal{P}_i \cap k[X_{n-d+1}, \ldots, X_n])$ -module de type fini. Or ce dernier anneau est lui-même un $k[X'_{n-d'+1}, \ldots, X'_n]$-module de type fini (3.2.1).

Au total $k[X'_1, \ldots, X'_n]/\overline{\tau}'(\mathcal{P}_i)$ est un $k[X'_{n-d'+1}, \ldots, X'_n]$-module de type fini et une $k[X'_{n-d'+1}, \ldots, X'_n]$-algèbre entière. Comme ci-dessus, on montre que d' est le degré de transcendance du corps des fractions de $k[X'_1, \ldots, X'_n]/\overline{\tau}'(\mathcal{P}_i)$ sur k , c'est donc aussi le degré de transcendance de K_i sur k .

6.5.0. REMARQUE. — Soit I un idéal de $k[X_1, \ldots, X_n] \neq (1)$, $\neq (0)$ et d un entier tel que $0 \leq d < n$. Si $k[X_1, \ldots, X_n]/I$ est une $k[X_{n-d+1}, \ldots, X_n]$-algèbre entière et si d est la k-dimension de $V(I)$, alors $k[X_{n-d+1}, \ldots, X_n] \to k[X_1, \ldots, X_n]/I$ est injective.

En effet, autrement il existerait $\tau : k[X_{n-d+1}, \ldots, X_n] \to k[X'_{n-d+1}, \ldots, X'_n]$ un changement de variables linéaire tel que les variables $X'_{n-d+1}, \ldots, X'_n$ soient commodes pour $\tau(I \cap k[X_{n-d+1}, \ldots, X_n])$. Etendant τ en $\overline{\tau} : k[X_1, \ldots, X_n] \to k[X'_1, \ldots, X'_n]$, $\overline{\tau}(X_i) = X_i$, $i = 1 \cdots n-d$, on obtiendrait comme ci-dessus l'existence de $\delta < d$ tel que $k[X'_1, \ldots, X'_n]/\overline{\tau}(I)$ est une $k[X'_{n-\delta+1}, \ldots, X'_n]$-algèbre entière et $k[X'_{n-\delta+1},\ldots,X'_n] \to k[X'_1,\ldots,X'_n]/\overline{\tau}(I)$ est injective et δ serait la k-dimension de $V(\overline{\tau}(I))$ et de $V(I)$.

6.5.1. COROLLAIRE. — *Soit I un idéal de $k[X_1,\ldots,X_n] \neq (1)$, $\neq (0)$. Si $\tau : k[X_1,\ldots,X_n] \to k[Y_1,\ldots,Y_n]$ est un changement de variables linéaire tel que les variables $Y_1,\ldots,Y_n$ soient commodes pour $\tau(I)$ et si d est un entier vérifiant i) et ii) de 5.2, d est la k-dimension de $V(I)$.*

Démonstration. — C'est une conséquence immédiate de 2.14, 2.14.1, de 5.3 et 6.5.

6.5.2. COROLLAIRE. — *Si I est un idéal de $k[X_1,\ldots,X_n] \neq (1)$, la k- dimension de $V(I)$ coincide avec sa dimension géométrique. Nous appellerons désormais cet entier la dimension de $V(I)$ et le noterons $\dim V(I)$. Il est compris entre 0 et $n-1$ si $I \neq (0)$. Il vaut n si $I = (0)$.*

Démonstration. — C'est une conséquence immédiate de 5.6 et 6.5.1.

6.5.3. REMARQUE. — L'énoncé de 6.5.2 reste valable si k n'est pas un corps infini. Nous admettrons ce résultat.

6.5.4. COROLLAIRE. — *Si I est un idéal de $k[X_1,\ldots,X_n] \neq (1)$, $\neq (0)$,$\dim V(I) = \dim V(\operatorname{gr} I)$.*

Démonstration. — C'est une conséquence immédiate de 6.5, 5.2 et 5.3. Remarquer que les composantes irréductibles de $V(\operatorname{gr} I)$ ne s'obtiennent pas directement à partir de celles de $V(I)$.

6.5.5. COROLLAIRE. — *Les hypothèses et notations étant celles de 6.5.1, pour tout $y_{n-d+1},\ldots,y_n \in \overline{k}^d$, $V(I) \cap \bigcap_{i=n-d+1,\ldots,n} V(\tau^{-1}(Y_i - y_i))$ est un ensemble fini non vide.*

Démonstration. — Compte tenu de 5.3, c'est une reformulation de 5.8. La notion de variables commodes généralise, mutatis mutandis, la notion de variables non principales pour les systèmes linéaires.

6.5.6. REMARQUE. — Les conditions suivantes sont équivalentes :

i) $V(I) = \overline{k}^n$;

ii) $\dim V(I) = n$;

iii) $I = (0)$.

Démonstration. — *i)* $\Rightarrow$ *ii)* à cause de 6.5.5; *ii)* $\Rightarrow$ *iii)* , 6.5.2; *iii)* $\Rightarrow$ *i)* , évident.

6.5.7. REMARQUE. — Les conditions suivantes sont équivalentes :

i) $V(I)$ est un ensemble fini non vide;

ii) $\dim V(I) = 0$;

iii) $1 \leq \mathrm{rg}_k k[X_1, \ldots, X_n]/I < \infty$.

Démonstration. — *i)* $\Rightarrow$ *ii)* à cause de 6.5.5; *ii)* $\Rightarrow$ *iii)* à cause de 6.5.1 et 5.3, *iii)* $\Rightarrow$ *i)* , 1.4.

7. Dimension et polynôme de Hilbert

Nous allons montrer dans ce paragraphe que $\dim V(I)$ peut se lire directement sur $\exp I$ l'ensemble des exposants privilégiés de I pour *l'ordre diagonal.*

7.1. LEMME. — *Soit k un corps et H un idéal homogène $\neq (0)$ dans $k[X_1,\ldots,X_n]$. Soit $\exp H$ l'ensemble des exposants privilégiés de H pour un ordre total sur $\mathbf{N}^n$ vérifiant I.1.1. Soit $k[X_1,\ldots,X_n]_s$ l'ensemble des polynômes homogènes de degré s et soit $H_s = H \cap k[X_1,\ldots,X_n]_s$.*

Soit $F_s = \{\alpha\ ,\ \alpha \in \mathbf{N}^n\ ,\ |\alpha| = s\ ,\ \alpha \notin \exp H\}\ ,\ s \in \mathbf{N}$

$$\operatorname{rg}_k k[X_1,\ldots,X_n]_s/H_s = \sharp F_s\ ,\ \forall s \in \mathbf{N}.$$

Démonstration. — $(\operatorname{cl} X^\alpha \operatorname{mod} H_s)_{\alpha\in F_s}$ est une base de $k[X_1,\ldots,X_n]_s/H_s$. En effet, si $f = \sum_{\alpha\in F_s} c_\alpha X^\alpha \in H_s$ et si $f \neq 0$, $\exp f \in \exp H \cap F_s = \emptyset$. C'est donc que $f = 0$ et que les éléments ci-dessus sont linéairement indépendants. Soit maintenant $f \in k[X_1,\ldots,X_n]_s$; il existe $g \in H$ tel que $f = g + fRH$ et si $fRH = \sum c_\alpha X^\alpha$, $c_\alpha \neq 0 \Rightarrow \alpha \notin \exp H$ (I.2.7). Soit g_s la partie homogène de degré s de g , $g_s \in H_s$ et $f = g_s + \sum_{|\alpha|=s} c_\alpha X^\alpha$. Les mêmes éléments engendrent donc $k[X_1,\ldots,X_n]_s/H_s$.

7.2. DÉFINITION. — *Soit E un E-sous ensemble de $\mathbf{N}^n$ non vide et $\neq \mathbf{N}^n$. Soit $\alpha_1,\ldots,\alpha_t$ l'escalier de E (I.1.8). Soit $\alpha_k = (\alpha_{k1},\ldots,\alpha_{kn})$, $k = 1\cdots t$. Soit $J_k = \{i \in (1\cdots n)\ ,\ \alpha_{ki} \neq 0\}$. $J_k \neq \emptyset$, $k = 1\cdots t$ car $E \neq \mathbf{N}^n$. Soit $\Im = \{I \subset (1\cdots n)\ ,\ I \cap J_k \neq \emptyset\ ,\ k = 1\cdots t\}$, $\Im \neq \emptyset$ puisque $(1\cdots n) \in \Im$ et si $I_1 \in \Im$ et $I_1 \subset I_2$, $I_2 \in \Im$. Soit $d = n - \inf_{I\in\Im} \sharp I$. d est appelé la dimension du E-sous ensemble E . Puisque $I \in \Im$ implique $I \neq \emptyset$, $0 \leq d \leq n-1$.*

Cette définition est justifiée par la remarque suivante :

7.3. REMARQUE. — k étant un corps quelconque, soit $H_k(E)$ l'idéal de $k[X_1,\ldots,X_n]$ engendré par $X^{\alpha_1},\ldots,X^{\alpha_t}$. Soit $H_j = V(X_j)$, $j = 1\cdots n$. On a $V(X^{\alpha_j}) = \cup_{i\in J_j} H_i$, $j = 1\cdots t$. Pour tout $I \subset (1\cdots n)$, soit $E_I = \cap_{i\in I} H_i$. $(e_1,\ldots,e_n)$ étant la base canonique de $\overline{k}^n$, E_I est le sous-espace vectoriel de $\overline{k}^n$ engendré par $(e_j)_{j\notin I}$ et son rang est $n - \sharp I$. On a

$$V(H_k(E)) = \bigcup_{I\in\Im} E_I = \bigcup_{I \mathrm{minimaux dans} \Im} E_I.$$

$V(H_k(E))$ est donc une réunion finie de $\overline{k}$-espaces vectoriels de rang inférieur ou égal à d , l'un d'eux ayant le rang d exactement.

7.4. PROPOSITION. — *Soit E un E-sous ensemble de $\mathbf{N}^n$ non vide et $\neq \mathbf{N}^n$. Pour tout $s \in \mathbf{N}$, soit $F_s = \{\alpha \in \mathbf{N}^n\ ,\ |\alpha| = s\ ,\ \alpha \notin E\}$. d étant la* *dimension de E , il existe un polynôme $P(T) \in \mathbf{Q}[T]$ de degré $d-1$ et un entier N (dépendant de E) tel que si $s \geq N$*

$$\sharp F_s = P(s)$$

(si $d = 0$, l'assertion signifie $P(T) \equiv 0$ et $F_s = \emptyset$ si $s \geq N$).

Démonstration. — Par récurrence sur n . Si $n = 1$, E étant un E-sous ensemble non vide de $\mathbf{N}$, $\neq \mathbf{N}$, il existe un entier $N > 0$ tel que $E = \{\alpha \in \mathbf{N}, \alpha \geq N\}$. On a alors $F_s = \emptyset$ si $s \geq N$, $P(T) \equiv 0$. La dimension de E est 0.

Supposons le résultat montré pour tout E-sous ensemble de $\mathbf{N}^k$ non vide et $\neq \mathbf{N}^k$, $k = 1 \cdots n-1$. Soit E un E-sous ensemble de $\mathbf{N}^n$ non vide, $\neq \mathbf{N}^n$. Soit $H = H_{\mathbf{C}}(E)$. H étant engendré par des monômes est a fortiori un idéal homogène de $\mathbf{C}[X_1, \ldots, X_n] \neq (0)$, $\neq (1)$. Pour tout ordre total sur $\mathbf{N}^n$ vérifiant I.1.1, $\exp H = E$. En effet, si $\alpha \in E$, $\exists k$, $1 \leq k \leq t$ et $\beta \in \mathbf{N}^n$, $\alpha = \alpha_k + \beta$; $X^\alpha \in H$; $\alpha = \exp X^\alpha \in \exp H$ et $E \subset \exp H$. Réciproquement, si $\alpha \in \exp H$, il existe $g \in H$ tel que $\alpha = \exp g$. X^α est donc un monôme de g . Mais H étant engendré par des monômes, $X^\alpha \in H$ et il existe k , $1 \leq k \leq t$ et $\beta \in \mathbf{N}^n$, $X^\alpha = X^\beta \cdot X^{\alpha_k}$ et $\alpha \in E$.

D'après 7.1, on a donc :

$$\sharp F_s = \mathrm{rg}_{\mathbf{C}} \mathbf{C}[X_1, \ldots, X_n]_s / H_s.$$

D'autre part (7.3) $V(H) = \cup_{i=1 \cdots u} G_i$, G_i étant un $\mathbf{C}$- espace vectoriel de rang inférieur ou égal à d et il existe i_0 , $1 \leq i_0 \leq u$, tel que $\mathrm{rg}_{\mathbf{C}} G_{i_0} = d$. Soit F un sous-espace vectoriel de $\mathbf{C}^n$ de rang $n-d$ tel que $F \cap G_i = 0$, $i = 1 \cdots u$, $F \cap V(H) = 0$. Soit $\pi : \mathbf{C}^n \to \mathbf{C}^n$, $\pi(x'_1, \ldots, x'_n) = (\ldots, L_i(x'_1, \ldots, x'_n), \ldots)$ l'application linéaire tel que $e'_1, \ldots, e'_n$ étant la base canonique du $\mathbf{C}^n$-source, $\pi(\oplus_{i=1 \cdots n-d} \mathbf{C}e'_i) = F$, $\pi(\oplus_{i=n-d+1, \ldots, n} \mathbf{C}e'_i) = G_{i_0}$ et soit $\tau : \mathbf{C}[X_1, \ldots, X_n] \to \mathbf{C}[X'_1, \ldots, X'_n]$ tel que $\tau(X_i) = L_i(X'_1, \ldots, X'_n)$, $i = 1 \cdots n$, le changement de variables linéaire correspondant.

Soit $H' = \tau(H)$. H' est un idéal homogène de $\mathbf{C}[X'_1, \ldots, X'_n]$(mais il n'est plus engendré par des monômes).

$$\begin{aligned} V(H') \cap V(X'_{n-d+1}) \cap \cdots \cap V(X'_n) &= V(H') \cap \oplus_{i=1 \cdots n-d} \mathbf{C}e'_i \\ &= \pi^{-1}(V(H)) \cap \pi^{-1}(F) = \pi^{-1}(V(H) \cap F) = \pi^{-1}(0) = 0. \end{aligned}$$

Comme $H' \neq (1)$, (5.4), $\mathbf{C}[X'_1, \ldots, X'_n]/H'$ est une $\mathbf{C}[X'_{n-d+1}, \ldots, X'_n]$-algèbre entière.

De plus $\mathbf{C}[X'_{n-d+1}, \ldots, X'_n] \cap H' = 0$. En effet

$$V(H') = \pi^{-1}(V(H)) \supset \pi^{-1}(G_{i_0}) = \bigoplus_{i=n-d+1, \ldots, n} \mathbf{C}e'_i.$$

Si donc

$$f \in \mathbf{C}[X'_{n-d+1}, \ldots, X'_n] \cap H' \text{ , } f(x'_{n-d+1}, \ldots, x'_n) = 0 \text{ , } \forall (x'_{n-d+1}, \ldots, x'_n) \in \mathbf{C}^d.$$

Donc $f = 0$. Les variables $X'_1, \ldots, X'_n$ sont donc commodes pour H' (5.2) ($H' = \operatorname{gr} H'$) et $d = \dim V(H')$ (6.5,6.5.2).

Soit $E' = \exp H'$ l'ensemble des privilégiés de H' pour l'ordre diagonal (I.1.1.2.1).

D'une part, τ étant un changement de variables linéaire,

$$\operatorname{rg}_{\mathbf{C}} \mathbf{C}[X_1, \ldots, X_n]_s / H_s = \operatorname{rg}_{\mathbf{C}} \mathbf{C}[X'_1, \ldots, X'_n]_s / H'_s$$

d'autre part (7.1)

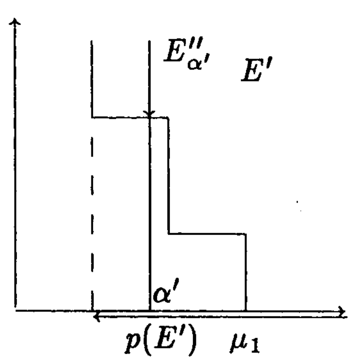
$$\operatorname{rg}_{\mathbf{C}} \mathbf{C}[X'_1, \ldots, X'_n]_s / H'_s = \sharp F'_s$$

où $F'_s = \{\alpha \, , \, \alpha \in \mathbf{N}^n \, , \, |\alpha| = s \, , \, \alpha \notin E'\}$ et $\sharp F_s = \sharp F'_s$.

Considérons $\mathbf{N}^n - E'$. Soit $p : \mathbf{N}^n \to \mathbf{N}^{n-d}$ la projection sur les $n-d$ premiers facteurs. $X'_1, \ldots, X'_n$ étant commodes pour H' , $\forall j = 1 \cdots n-d, \exists \mu_j$, $\mu_j \in \mathbf{N}$, $\mu_j \geq 1$, tel que $X'^{\mu_j}_j \in \operatorname{in} H'$ (5.5). Donc $(0, \ldots, \mu_j, \ldots, 0) \in E'$ (μ_j à la j-ième place) $j = 1 \cdots n-d$ et $(0, \ldots, \mu_j, \ldots, 0) \in p(E')$, $j = 1 \cdots n-d$. $p(E')$ est un E- sous ensemble non vide de $\mathbf{N}^{n-d}$. Egalement $p(E') \neq \mathbf{N}^{n-d}$.(En effet, autrement, il existerait $\alpha_{n-d+1}, \ldots, \alpha_n \in \mathbf{N}^d$ tel que $X'^{\alpha_{n-d+1}}_{n-d+1} \cdots X'^{\alpha_n}_n \in \operatorname{in} H'$. H' étant homogène, il existerait $h' \in H'$ homogène de degré $\sum \alpha_i$ tel que $\operatorname{in} h' = X'^{\alpha_{n-d+1}}_{n-d+1} \cdots X'^{\alpha_n}_n$ et l'ordre étant diagonal, (*cf.* I.4.1) $h' \in \mathbf{C}[X'_{n-d+1}, \ldots, X'_n]$. Or $H' \cap \mathbf{C}[X'_{n-d+1}, \ldots, X'_n] = 0$) . $\mathbf{N}^{n-d} - p(E')$ est donc un ensemble fini non vide. Son cardinal est majoré par $\mu_1 \cdots \mu_{n-d}$.

7.4.0. LEMME. —

$$\mathbf{N}^n - E' = \mathbf{N}^{n-d} - p(E') \times \mathbf{N}^d \cup \bigcup_{\substack{\alpha' \in p(E') \\ \alpha'_i < \mu_i \, , \, i = 1 \cdots n-d}} (\alpha' \times \mathbf{N}^d) \cap \mathbf{N}^n - E'.$$



Considérons d'abord $\alpha = (\alpha_1, \ldots, \alpha_{n-d}, \alpha_{n-d+1}, \ldots, \alpha_n) \notin E'$ ou bien $p(\alpha) \notin p(E')$ ou bien $p(\alpha) \in p(E')$. Alors $\alpha_i < \mu_i$, $i = 1 \cdots n-d$. Autrement, il existerait $i_0 \in 1 \cdots n-d$ tel que $\alpha_{i_0} \geq \mu_{i_0}$. Or $(0, \ldots, \mu_{i_0}, \ldots, 0) \in E'$ et E' étant un E-ensemble, $\alpha \in E'$ contrairement à l'hypothèse.

Si maintenant $p(\alpha) \notin p(E')$, $\alpha \notin E'$.

Or si $\alpha' \in p(E')$, $E''_{\alpha'} = \{\alpha'' \in \mathbf{N}^d \, , \, (\alpha', \alpha'') \in E'\}$ est un E-sous ensemble de $\mathbf{N}^d$ non vide et $\alpha' \times \mathbf{N}^d \cap \mathbf{N}^n - E' = \alpha' \times \mathbf{N}^d - E''_{\alpha'}$. Finalement

$$\mathbf{N}^n - E' = \mathbf{N}^{n-d} - p(E') \times \mathbf{N}^d \cup \bigcup_{\substack{\alpha' \in p(E') \\ \alpha'_i < \mu_i \, , \, i = 1 \cdots n-d}} \alpha' \times \mathbf{N}^d - E''_{\alpha'}.$$

Il en résulte que si $s \geq \mu_1 + \cdots + \mu_{n-d}$,

$$\sharp F'_s = \sum_{\alpha' \in \mathbf{N}^{n-d} - p(E')} \mathrm{rg}_{\mathbf{C}} \mathbf{C}[X'_{n-d+1}, \dots, X'_n]_{s-|\alpha'|} + \sum_{\substack{\alpha' \in p(E') \\ \alpha'_i < \mu_i \ , \ i=1\cdots n-d}} \sharp F''_{\alpha', s-|\alpha'|}$$

où $\forall t \in \mathbf{N}$, $F''_{\alpha',t} = \{\alpha'' \in \mathbf{N}^d \ , \ |\alpha''| = t \ , \ \alpha'' \notin E''_{\alpha'}\}$.

Or $\mathrm{rg}_{\mathbf{C}} \mathbf{C}[X'_{n-d+1}, \dots, X'_n]_{s-|\alpha'|} = \binom{s-|\alpha'|+d-1}{d-1}$. Soit

$$R(T) = \frac{(T+d-1)\cdots(T+1)}{(d-1)!} \in \mathbf{Q}[T].$$

C'est un polynôme de degré $d-1$ dont le coefficient du terme dominant est $1/(d-1)!$. Puisque $d \leq n-1$, on peut appliquer l'hypothèse de récurrence à $E''_{\alpha'}$. Pour tout $\alpha' \in p(E')$,$\alpha'_i < \mu_i$, $i = 1 \cdots n-d$, tel que $E''_{\alpha'} \neq \mathbf{N}^d$, il existe $N_{\alpha'} \in \mathbf{N}$ et $Q_{\alpha'} \in \mathbf{Q}[T]$ un polynôme de degré $d_{\alpha'} - 1 = \dim E''_{\alpha'} - 1$ tel que si $t \geq N_{\alpha'}$, $\sharp F''_{\alpha',t} = Q_{\alpha'}(t)$. Or $d_{\alpha'} \leq d-1$. $Q_{\alpha'}$ est donc un polynôme de degré au plus $d-2$.

Si donc $s \geq \max_{\alpha' \in p(E'), \alpha'_i < \mu_i, i=1\cdots n-d, E''_{\alpha'} \neq \mathbf{N}^d} N_{\alpha'} + |\alpha'|$ et $s \geq \mu_1 + \cdots + \mu_d$

$$\sharp F'_s = \sum_{\alpha' \in \mathbf{N}^{n-d} - p(E')} R(s - |\alpha'|) + \sum_{\alpha' \in p(E'), \alpha'_i < \mu_i, i=1\cdots n-d, E''_{\alpha'} \neq \mathbf{N}^d} Q_{\alpha'}(s - |\alpha'|).$$

Puisque $p(E') \neq \mathbf{N}^{n-d}$, le premier $\sum$ est la valeur en s d'un polynôme de degré $d-1$ dont le terme dominant est $\sharp \mathbf{N}^{n-d} - p(E')/(d-1)!$, le deuxième $\sum$ la valeur en s d'un polynôme de degré au plus $d-2$ (tous deux à coefficients rationnels).

7.4.1. COROLLAIRE. — *Soit k un corps et H un idéal homogène de $k[X_1, \dots, X_n] \neq (1)$. Soit $d = \dim V(H)$. Il existe un polynôme $P(T) \in \mathbf{Q}[T]$ de degré $d-1$, dont le terme dominant est de la forme $m/(d-1)!$ où $m \in \mathbf{N}$, $m \geq 1$ et un entier N (dépendant de H) tel que si $s \geq N$,*

$$\mathrm{rg}_k k[X_1, \dots, X_n]_s / H_s = P(s).$$

Démonstration. — Si $H = 0$, $\dim V(H) = n$, $P(T) = \binom{T+n-1}{n-1}, N = 0$ conviennent. Si $H \neq (0)$, on peut supposer k infini ou même algébriquement clos puisque $\mathrm{rg}_k k[X_1, \dots, X_n]_s / H_s = \mathrm{rg}_{\overline{k}} \overline{k}[X_1, \dots, X_n]_s / \overline{H}_s$. Soit alors τ : $k[X_1, \dots, X_n] \to k[X'_1, \dots, X'_n]$ un changement de variables linéaire tel que les variables $X'_1, \dots, X'_n$ soient commodes pour $\tau(H)$. Soit $H' = \tau(H)$; H' est un idéal homogène $\neq (0)$.

$$\forall s \in \mathbf{N}, \mathrm{rg}_k k[X_1, \dots, X_n]_s / H_s = \mathrm{rg}_k k[X'_1, \dots, X'_n]_s / H'_s.$$

Soit $E' = \exp H'$ l'ensemble des privilégiés de H' pour l'ordre diagonal. D'après 7.1,

$$\forall s \in \mathbf{N} \ , \ \mathrm{rg}_k k[X'_1, \dots, X'_n] / H'_s = \sharp F'_s$$

où $F'_s = \{\alpha \in \mathbf{N}^n, |\alpha| = s, \alpha \notin E'\}$. D'après 7.4, il existe donc $P(T) \in \mathbf{Q}[T]$ de degré $\delta - 1$ (où δ est la dimension de E') et $N \in \mathbf{N}$ tel que si $s \geq \mathbf{N}$, $\sharp F'_s = P(s)$. Il suffit donc de montrer que $\delta = d$. Or $H_k(E') = \text{in } H'$ par définition. Déterminons $V(\text{in } H')$. D'après 6.5.1, d est l'entier vérifiant *i)* et *ii)* de 5.2. D'après 5.5, $\forall j$, $j = 1 \cdots n-d$, $\exists \mu_j \in \mathbf{N}$, $\mu_j \geq 1$ tel que $X'^{\mu_j}_j \in \text{in } H'$. Donc $(X'^{\mu_1}_1, \ldots, X'^{\mu_{n-d}}_{n-d}) \subset$ in H' . D'autre part soit $X'^{\theta} \in \text{in } H'$. Il existe i , $1 \leq i \leq n-d$ tel que $\theta_i \neq 0$, autrement $X'^{\theta} \in \text{in } H' \cap k[X'_{n-d+1}, \ldots, X'_n]$. Alors H' étant homogène et l'ordre étant l'ordre diagonal, il existerait $h' \in H' \cap k[X'_{n-d+1}, \ldots, X'_n]_{|\theta|}$ tel que in $h' = X'^{\theta}$ (*cf.* I.4.1). Or $H' \cap k[X'_{n-d+1}, \ldots, X'_n] = (0)$. C'est impossible. Donc in $H' \subset (X'_1, \ldots, X'_{n-d})$. $V(\text{in } H')$ est donc un k-espace vectoriel de rang d . Donc $\delta = d$ (7.3).

7.5. DÉFINITION. — *Sous les hypothèses de 7.4.1, $P(T)$ est appelé le polynôme de Hilbert de $k[X_1, \ldots, X_n]/H$.*

7.5.1. DÉFINITION. — *Sous les hypothèses de 7.4.1, le plus petit entier n tel que $\operatorname{rg}_k k[X_1, \ldots, X_n]_s/I_s = P(s)$, $\forall s \geq n$, est appelé l'indice de régularité de $k[X_1, \ldots, X_n]/I$.*

7.6. PROPOSITION. — *Soit I un idéal de $k[X_1, \ldots, X_n] \neq (1), \neq (0)$. Soit $\exp I$ l'ensemble des privilégiés de I pour l'ordre diagonal (I.1.1.2).*

$$\dim V(I) = \dim \exp I.$$

Démonstration. — On sait que $\dim V(I) = \dim V(\operatorname{gr} I)$ (6.5.4). Soit d cet entier. D'après 7.4.1, il existe $P(T) \in \mathbf{Q}[T]$ de degré $d-1$ tel que $\operatorname{rg}_k k[X_1, \ldots, X_n]_s/(\operatorname{gr} I)_s = P(s)$ pour s assez grand. D'après 7.1, $\operatorname{rg}_k k[X_1, \ldots, X_n]_s/(\operatorname{gr} I)_s = \sharp F_s$ où $F_s = \{\alpha \in \mathbf{N}^n , |\alpha| = s , \alpha \in \exp \operatorname{gr} I\}$. Or $E = \exp \operatorname{gr} I = \exp I$ (*cf.* 6.1). D'après 7.4, il existe $Q(T) \in \mathbf{Q}[T]$ de degré $\dim E - 1$ tel que $\sharp F_s = Q(s)$ pour s assez grand. Donc $P \equiv Q$ et $d-1 = \dim E - 1$. La dimension de $V(I)$ se lit donc directement sur $\exp I$ l'ensemble des privilégiés de I pour l'ordre diagonal sans avoir besoin d'effectuer de changement de variables.

7.6.1. REMARQUE. — L'énoncé précédent reste valable pour $\exp I$ l'ensemble des privilégiés de I pour l'ordre lexicographique inverse (I.1.1.2.2).

7.7. COROLLAIRE. — *Si I est un idéal principal de $k[X_1, \ldots, X_n]$, $\neq (1)$, $\neq (0)$, $\dim V(I) = n-1$.*

Démonstration. — Pour l'ordre diagonal (comme pour tout ordre) si $I = (f)$, $\exp I = (\exp f + \mathbf{N}^n)$. $\exp f$ est donc une frontière de $\exp I$. $V(\text{in } f) = V(H_k(\exp I))$ est une réunion de sous-espaces vectoriels de $\overline{k}^n$ de codim un et $\dim \exp I = n-1$.

7.8. COROLLAIRE. — *Soit H un idéal homogène de $k[X_1, \ldots, X_n] \neq (1)$ et $f \in k[X_1, \ldots, X_n]$ un polynôme homogène de degré $\mu \geq 1$*

$$\dim V(H) \geq \dim V(H+f) \geq \dim V(H) - 1.$$

Démonstration. — Soit $d = \dim V(H)$,$d' = \dim V(H+f)$. D'après 7.4.1, il existe $N \in \mathbf{N}$ et $P(T)$ (resp $Q(T)$) $\in \mathbf{Q}[T]$ tel que :

$$P(T) = \frac{m}{(d-1)!}T^{d-1} + \cdots (\text{resp}\, Q(T) = \frac{m'}{(d'-1)!}T^{d'-1} + \cdots) \ , \ m, m' \in \mathbf{N} \ , \ \geq 1,$$

et que :

$$\operatorname{rg}_k k[X_1, \ldots, X_n]_s/H_s = P(s) \, (\text{resp} \operatorname{rg}_k k[X_1, \ldots, X_n]_s/(H+f)_s = Q(s))$$

si $s \geq N$. Or, on a la suite exacte :

$$\begin{aligned} 0 \to K_s \to k[X_1, \ldots, X_n]_{s-\mu}/H_{s-\mu} &\xrightarrow{f} k[X_1, \ldots, X_n]_s/H_s \\ &\hookrightarrow k[X_1, \ldots, X_n]_s/(H+f)_s \to 0 \end{aligned}$$

(où la flèche notée f est la multiplication par f). On en déduit

$$\begin{aligned} &\operatorname{rg}_k k[X_1, \ldots, X_n]_s/(H+f)_s \\ &\qquad \geq \operatorname{rg}_k k[X_1, \ldots, X_n]_s/H_s - \operatorname{rg}_k k[X_1, \ldots, X_n]_{s-\mu}/H_{s-\mu} \end{aligned}$$

et si $s \geq N$

$$Q(s) \geq P(s) - P(s-\mu).$$

Or

$$\begin{aligned} P(s) - P(s-\mu) &= \frac{m}{(d-1)!}s^{d-1} - \frac{m}{(d-1)!}(s-\mu)^{d-1} + \sum_{j \leq d-2} r_j[s^j - (s-\mu)^j] \\ &= \frac{m\mu}{(d-2)!}s^{d-2} + \sum_{j \leq d-3} r'_j s^j \ , \ (r_j \in \mathbf{Q}). \end{aligned}$$

Il en résulte que : $d' - 1 \geq d - 2$ et $d' \geq d - 1$.

D'autre part, $\operatorname{rg}_k k[X_1, \ldots, X_n]_s/H_s \geq \operatorname{rg}_k k[X_1, \ldots, X_n]_s/(H+f)_s$ et si $s \geq N$, $P(s) \geq Q(s)$, donc $d - 1 \geq d' - 1$ et $d \geq d'$.

7.8.1. REMARQUE. — Si il existe $M \in \mathbf{N}$ tel que $K_s = 0$, si $s \geq M$, $\dim V(H+f) = \dim V(H) - 1$.

En effet, $Q(s) = \frac{m\mu}{(d-2)!}s^{d-2} + \sum_{j \leq d-3} r'_j s^j$ si s assez grand. Si cette condition est satisfaite, on dit que f est superficiel. Elle l'est en particulier si f est non diviseur de zéro dans $k[X_1, \ldots, X_n]/H$.

7.8.2. COROLLAIRE. — *Soit* $H = (f_1, \ldots, f_r)$, f_i *homogène,* $f_i \neq 0$ *dans* $k[X_1, \ldots, X_n]$, $\dim V(H) \geq n - r$.

7.8.3. REMARQUE. — L'analogue de 7.8 est faux, si on supprime les hypothèses d'homogénéité. Dans $k[X, Y, Z]$ soit $I = (ZX, ZY)$ et $f = Z + 1$, $\dim V(I) = 2$ $((ZX, ZY)$ est une base standard de I pour l'ordre diagonal et $\dim V(I) = \dim \exp I)$; $I + f = (ZX, ZY, Z+1) = (X, Y, Z+1)(X = X(Z+1) - ZX, Y = Y(Z+1) - ZY)$ et $\dim V(I+f) = 0$

Par contre, on peut démontrer que si $I \subset k[X_1, \ldots, X_n]$, $I = (f_1, \ldots, f_r)$, $V(I) \neq \emptyset$, $\dim V(I) \geq n - r$. Ceci nécessite la notion de localisation en géométrie algébrique.

7.9. PROPOSITION. — *Soit H un idéal homogène de $k[X_1,\ldots,X_n]$, $\neq (1)$. Soit $d = \dim V(H)$ et $\tau : k[X_1,\ldots,X_n] \to k[Y_1,\ldots,Y_n]$ un changement de variables linéaire tel que les variables $Y_1,\ldots,Y_n$ soient commodes pour $\tau(I)$. Alors*

$$\dim V\big(H + \tau^{-1}(Y_{n-d+1}) + \cdots + \tau^{-1}(Y_{n-d+i})\big) = d - i \ , \ i = 1 \cdots d.$$

Démonstration. — D'après 6.5.2, 6.5.5 et 6.5.7,

$$\dim V\big(H + \tau^{-1}(Y_{n-d+1}) + \cdots + \tau^{-1}(Y_n)\big) = 0.$$

L'assertion est alors une conséquence immédiate de 7.8.

1er exercice.

k étant un corps infini, soit I_1, I_2 2 idéaux de $k[X_1, \ldots, X_n]$ l'anneau des polynômes à n indéterminés sur k tels que $I_2 \neq (1)$ et $I_1 \subset I_2$. Soit $(f_1, \ldots, f_s)$ un système de générateurs de I_1 , $(f_1, \ldots, f_s, f_{s+1}, \ldots, f_{s+t})$ un système de générateurs de I_2 .

1) Utilisant l'algorithme de construction d'une base standard pour l'ordre diagonal d'un idéal à partir d'un système de générateurs, donner un algorithme de construction d'un changement de variables linéaire $\tau \, : \, k[X_1, \ldots, X_n] \to k[Y_1, \ldots, Y_n]$ tel que les variables $Y_1, \ldots, Y_n$ soient commodes pour $\tau(I_1)$ et $\tau(I_2)$ à partir des données $f_1, \ldots, f_{s+t}$.

2) En déduire que $\dim V(I_1) \geq \dim V(I_2)$.

3) On suppose I_1 premier et $\dim V(I_1) = \dim V(I_2)$. Montrer que $I_1 = I_2$. (On considèrera une relation de dépendance intégrale de $f \in k[Y_1, \ldots, Y_n]/\tau(I_1)$ sur $k[Y_{n-d+1}, \ldots, Y_n]$ si $d = \dim V(I_1)$, $f^s + g_1 f^{s-1} + \cdots + g_s = 0$ avec s minimal).

2ème exercice

k est un corps et $k[X, Y, Z]$ est l'anneau des polynômes à 3 indéterminées sur k .

Soit $f_1 = XZ - Y^2$, $f_2 = X^3 - YZ$, $f_3 = X^2Y - Z^2$.

1) Déterminer une base standard pour l'ordre diagonal de $I_2 = (f_1, f_2, f_3)$; en déduire une base du k-espace vectoriel $k[X, Y, Z]/I_2$.

2) Déterminer $V(\operatorname{gr} I_2)$, puis montrer que les variables X, Y, Z sont commodes pour I_2 . (Préciser l'entier d qui convient).

3) Soit $k[T]$ l'anneau des polynômes à 1 indéterminée sur k . Soit ϕ : $k[X, Y, Z]/I_2 \to k[T]$ l'application définie par :

$$\phi\Big(\mathrm{cl} \sum_{\alpha, \beta, \gamma \in \mathbf{N}^3} c_{\alpha\beta\gamma} X^\alpha Y^\beta Z^\gamma\Big) = \sum_{\alpha, \beta, \gamma} c_{\alpha\beta\gamma} T^{3\alpha + 4\beta + 5\gamma}.$$

Vérifier que ϕ est bien définie, puis montrer que ϕ est injective (on utilisera la base construite au 1)).

En déduire que I_2 est un idéal premier.

4) Soit $I_1 = (f_1, f_2)$; déterminer une base standard pour l'ordre diagonal de I_1 .

5) Comparer $V(\operatorname{gr} I_2)$ et $V(\operatorname{gr} I_1)$. Les variables X, Y, Z sont-elles commodes pour I_1 ?

6) Soit $k[T']$ l'anneau de polynômes à 1 indéterminée sur k . Soit ψ : $k[X,Y,Z]/I_1 \to k[T] \oplus k[T']$ l'application définie par :

$$\psi\,(\mathrm{cl}\,P(X,Y,Z)) = \phi(\mathrm{cl}\,P) + P(0,0,T').$$

Vérifier que ψ est bien définie, puis montrer que ψ est injective.

En déduire que $I_1 = I_2 \cap (X,Y)k[X,Y,Z]$.