CHAPITRE 7

DUALITÉ

Sommaire

Dans ce chapitre, nous allons étudier les formes linéaires sur l'anneau des polynômes, c'est-à-dire les éléments du dual de $\mathbb{K}[\mathbf{x}]$. Un thème de recherche connaissant depuis quelques temps des développements intéressants consiste à représenter les polynômes comme des « algorithmes » calculant une valeur en un point. On considère alors l'évaluation des polynômes en un point. Cette évaluation est une forme linéaire particulière. Nous voulons étendre donc ici ce point de vue en nous intéressant systématiquement aux propriétés des formes linéaires sur les polynômes.

7.1. Dualité et systèmes inverses

Dans cette section, nous allons décrire le dual de l'ensemble $R = \mathbb{K}[\mathbf{x}]$ des polynômes en $\mathbf{x}$, vu comme espace vectoriel sur $\mathbb{K}$.

7.1.1. Dualité et séries formelles. — Nous noterons $\widehat{R}$ l'espace vectoriel dual de R. Une forme linéaire « simple » de $\widehat{R}$ est l'*évaluation en un point* $\zeta \in \mathbb{K}^n$,

$$\begin{array}{rccl} \mathbf{1}_\zeta : & R & \to & \mathbb{K} \\ & p & \mapsto & \mathbf{1}_\zeta(p) = p(\zeta). \end{array}$$

Pour tout multi-indice $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, on peut aussi considérer la forme linéaire

$$\begin{array}{rccl} \delta_\zeta^\alpha : & R & \to & \mathbb{K} \\ & p & \mapsto & \delta_\zeta^\alpha(p) = \partial_{x_1}^{\alpha_1} \cdots \partial_{x_n}^{\alpha_n}(p)(\zeta), \end{array}$$

où ∂_{x_i} désigne la dérivation par rapport à la variable x_i. Nous notons, $\delta_{i,\zeta} = \partial_\zeta^\alpha$, avec $\alpha_i = 1$ et $\alpha_j = 0, j \neq i$. Avec ces notations, $\delta_\zeta^\alpha = \delta_{1,\zeta}^{\alpha_1} \cdots \delta_{n,\zeta}^{\alpha_n}$.

***Exemple* 7.1.** *Pour* $\zeta = (1,1) \in \mathbb{R}^2$ *et* $p = x^2 + 2\,x\,y - 3\,y^2 + x - y + 1 \in \mathbb{R}[x,y]$, $\mathbf{1}_\zeta(p) = 1, \delta_\zeta^{(0,2)}(p) = -6$.

Pour tout $f \in \mathbb{K}[x_1, \ldots, x_n]$, notons $(\mathbf{d}_\zeta^\alpha(f))_{\alpha \in \mathbb{N}^n}$ les coefficients de f dans la base $((\mathbf{x} - \zeta)^\alpha)_{\alpha \in \mathbb{N}^n}$. On a alors

$$f(\mathbf{x}) = \sum_{\alpha \in \mathbb{N}^n} \mathbf{d}_\zeta^\alpha(f)(\mathbf{x} - \zeta)^\alpha,$$

où $(\mathbf{x} - \zeta)^\alpha = \prod_{i=1}^n (x_i - \zeta_i)^{\alpha_i}$. Notons que si la caractéristique de $\mathbb{K}$ est nulle, $\mathbf{d}_\zeta^\alpha = \mathbf{d}_{1,\zeta}^{\alpha_1} \cdots \mathbf{d}_{n,\zeta}^{\alpha_n} = \frac{1}{\prod_{i=1}^n \alpha_i!}\, \delta_\zeta^\alpha = \frac{1}{\alpha!}\, \delta_\zeta^\alpha$. Pour toute forme linéaire Λ sur R, on a donc

$$\Lambda(f) = \sum_{\alpha \in \mathbb{N}^n} \Lambda((\mathbf{x} - \zeta)^\alpha)\, \mathbf{d}_\zeta^\alpha(f).$$

Par conséquent,

$$\Lambda = \sum_{\alpha\in\mathbb{N}^n} \Lambda((\mathbf{x}-\zeta)^\alpha)\,\mathbf{d}_\zeta^\alpha.$$

Ce qui nous permet d'identifier Λ avec la série formelle $\sum_{\alpha\in\mathbb{N}^n} \Lambda((\mathbf{x}-\zeta)^\alpha)\mathbf{d}_\zeta^\alpha \in \mathbb{K}[[\mathbf{d}_{1,\zeta},\dots \mathbf{d}_{n,\zeta}]]$. Si la caractéristique de $\mathbb{K}$ est 0, cette identification est réalisée par le développement de Taylor en ζ.

$$\Lambda = \sum_{\alpha\in\mathbb{N}^n} \Lambda((\mathbf{x}-\zeta)^\alpha)\,\frac{1}{\alpha!}\,\delta_\zeta^\alpha \in \mathbb{K}[[\delta_{1,\zeta},\dots \delta_{n,\zeta}]].$$

Lorsque $\zeta = 0, \mathbf{d}_\zeta^\alpha$ sera noté $\mathbf{d}^\alpha$. Par la suite, nous noterons également $\mathbf{d}_\zeta^\alpha(p) = \langle \mathbf{d}^\alpha, p\rangle_\zeta$.

***Exemple* 7.2.** *Considérons l'application linéaire* $\Lambda : p \in \mathbb{R}[x] \mapsto \int_0^2 p(x)dx$. *Comme* $\int_0^2 x^i dx = \frac{2^{i+1}}{i+1} (i \in \mathbb{N})$, *nous pouvons réécrire* Λ *en série formelle sous la forme :*

$$\Lambda = \sum_{i\geq 0} \frac{2^{i+1}}{i+1}\mathbf{d}^i = \sum_{i\geq 1} \frac{2^i}{i}\mathbf{d}^{i-1},$$

où $\mathbf{d}^i : p \mapsto \frac{1}{i!}\partial^i(p)(0)$ *est la forme linéaire qui donne le coefficient de* x^i *d'un polynôme* p.

Via ce formalisme, *l'algèbre* $\mathbb{K}[[\delta_{1,\zeta},\dots,\delta_{n,\zeta}]]$ *des séries formelles* (*ou opérateurs différentiels « en* ζ *» à coefficients dans* $\mathbb{K}$) *ou* $\mathbb{K}[[\mathbf{d}_{1,\zeta},\dots \mathbf{d}_{n,\zeta}]]$ *s'identifie à* $\widehat{R}$. Cette identification est réalisée par le développement de Taylor en ζ.

On vérifie facilement que

$$\langle \mathbf{d}^\alpha, (\mathbf{x}-\zeta)^\beta\rangle_\zeta = \begin{cases} 1 \text{ si } \ \alpha = \beta, \\ 0 \text{ sinon.} \end{cases}$$

La base $(\mathbf{d}_\zeta^\alpha)_{\alpha\in\mathbb{N}^n}$ de $\widehat{R}$ est donc la base duale de la base monomiale $((\mathbf{x}-\zeta)^\alpha)_{\alpha\in\mathbb{N}^n}$ de R. Voir [**Ems78**] pour plus de détail.

Remarquons que l'on peut aussi choisir comme base de $\widehat{R}$, $(\mathbf{1}_\zeta)_{\zeta\in\mathcal{P}}$ où $\mathcal{P}$ est un ensemble infini de points convenablement choisis.

A partir de maintenant, nous allons identifier $\widehat{R}$ avec $\mathbb{K}[[\mathbf{d}_{1,\zeta},\dots,\mathbf{d}_{n,\zeta}]]$ (resp. $= \mathbb{K}[[\delta_{1,\zeta},\dots,\delta_{n,\zeta}]]$ si $\mathrm{car}(\mathbb{K}) = 0$). Les formes linéaires seront donc vues comme

- des séries formelles en $\mathbf{d}_{1,\zeta},\dots,\mathbf{d}_{n,\zeta}$,
- ou même *comme des opérateurs différentiels au point* ζ, qui sont des séries formelles en $\delta_{1,\zeta},\dots,\delta_{n,\zeta}$.

On notera aussi leur espace $\mathbb{K}[[\mathbf{d}_\zeta]]$ (resp. $\mathbb{K}[[\delta_\zeta]]$ si $\mathrm{car}(\mathbb{K}) = 0$). Lorsque $\zeta = 0, \mathbb{K}[[\mathbf{d}_\zeta]]$ sera noté $\mathbb{K}[[\mathbf{d}_1,\dots,\mathbf{d}_n]]$ (resp. $\mathbb{K}[[\delta_1,\dots,\delta_n]]$) ou $\mathbb{K}[[\mathbf{d}]]$ (resp. $\mathbb{K}[[\delta]]$ si $\mathrm{car}(\mathbb{K}) = 0$).

7.1.2. Dualité et dérivation. — L'espace vectoriel $\widehat{R}$ est muni d'une structure de R-module de la façon suivante : $\forall p \in R$, $\forall \Lambda \in \widehat{R}$, on définit $p \cdot \Lambda$ par

$$\begin{aligned} p \cdot \Lambda : R &\to \mathbb{K} \\ q &\mapsto \Lambda(p\,q). \end{aligned}$$

Montrons que cette opération correspond dans $\mathbb{K}[[\delta_\zeta]]$ à des dérivations. En effet, on a par récurrence sur $a \in \mathbb{N}^*$,

$$\partial^a_{x_i}((x_i - \zeta_i)\,p) = a\,\partial^{a-1}_{x_i}(p) + (x_i - \zeta_i)\,\partial^a_{x_i}(p).$$

Ce qui implique que

$$\begin{aligned} (x_i - \zeta_i) \cdot \delta^\alpha_\zeta(p) &= \delta^\alpha_\zeta((x_i - \zeta_i)\,p) \\ &= \alpha_i \delta^{\alpha_1}_{1,\zeta} \cdots \delta^{\alpha_{i-1}}_{i-1,\zeta} \delta^{\alpha_i - 1}_{i,\zeta} \delta^{\alpha_{i+1}}_{i+1,\zeta} \cdots \delta^{\alpha_n}_{n,\zeta}(p) \\ &= \partial_{\delta_{i,\zeta}}(\delta^\alpha_\zeta)(p). \end{aligned}$$

Donc la multiplication par $x_i - \zeta_i$ dans $\widehat{R}$ agit sur les éléments de $\mathbb{K}[[\delta_\zeta]]$ comme une dérivation par rapport à la variable $\delta_{i,\zeta}$.

Nous vérifions également que la multiplication par $x_i - \zeta_i$ dans $\widehat{R}$ agit sur les éléments de $\mathbb{K}[[\mathbf{d}_\zeta]]$ comme la multiplication par « l'inverse de la variable $\delta_{i,\zeta}$ ». En effet, comme $\mathbf{d}^\alpha_\zeta = \frac{1}{\alpha!}\,\delta^\alpha_\zeta$, on a

$$(x_i - \zeta_i) \cdot \mathbf{d}^\alpha_\zeta = \mathbf{d}^{\alpha_1}_{1,\zeta} \cdots \mathbf{d}^{\alpha_{i-1}}_{i-1,\zeta} \mathbf{d}^{\alpha_i - 1}_{i,\zeta} \mathbf{d}^{\alpha_{i+1}}_{i+1,\zeta} \cdots \mathbf{d}^{\alpha_n}_{n,\zeta}$$

et $x_i - \zeta_i$ est « équivalent » à $\mathbf{d}^{-1}_{i,\zeta}$. Ce qui explique l'appellation de système inverse [**Mac16**].

***Exemple* 7.3.** *Dans* $\mathbb{K}[x_1, x_2]$, $x_1 \cdot \mathbf{d}^2_1\mathbf{d}_2 : p \in \mathbb{K}[x_1, x_2] \mapsto$ *le coefficient de* $x^2_1 x_2$ *dans* $x_1 p$, *c'est donc le coefficient* $\mathbf{d}_1\mathbf{d}_2(p)$ *de* $x_1 x_2$ *dans* p. *On a bien* $x_1 \cdot \mathbf{d}^2_1\mathbf{d}_2 = \mathbf{d}^{-1}_1\mathbf{d}^2_1\mathbf{d}_2 = \mathbf{d}_1\mathbf{d}_2$.

7.1.3. Changement de base. — Décrivons ici, comment on peut passer des opérateurs différentiels en ζ aux opérateurs différentiels en un autre point. Pour simplifier la présentation, nous supposons que $\mathrm{car}(\mathbb{K}) = 0$.

***Définition* 7.4.** *Notons*

$$\Delta(\zeta, \delta) = \sum_{\alpha \in \mathbb{N}^n} \frac{1}{\alpha!} \zeta^\alpha \delta^\alpha.$$

Nous allons définir l'isomorphisme entre $\mathbb{K}[[\delta_\zeta]]$ et $\mathbb{K}[[\delta]]$. Tout autre changement de points induit le même type d'isomorphisme (à translation près).

***Théorème* 7.5.** *L'isomorphisme de passage de* $\mathbb{K}[[\delta_\zeta]]$ *à* $\mathbb{K}[[\delta]]$ *induit par l'isomorphisme entre* $\widehat{R}$ *et* $\mathbb{K}[[\delta_\zeta]]$ *et celui entre* $\widehat{R}$ *et* $\mathbb{K}[[\delta]]$ *est donné par*

$$\begin{array}{rcl} \mathbb{K}[[\delta_\zeta]] & \to & \mathbb{K}[[\delta]] \\ \delta_\zeta^\alpha & \mapsto & \delta^\alpha\, \Delta(\zeta,\delta). \end{array}$$

Démonstration. Pour tout $p = \sum_{\alpha\in\mathbb{N}^n} p_\alpha\, \mathbf{x}^\alpha \in R$ et tout $\beta = (\beta_1,\ldots,\beta_n) \in \mathbb{N}^n$, notons $p^{(\beta)} = \partial_{x_1}^{\beta_1}\cdots\partial_{x_n}^{\beta_n}(p) = \sum_{\alpha\in\mathbb{N}^n} p_\alpha^{(\beta)}\mathbf{x}^\alpha$. On a donc

$$\begin{array}{rcl} \delta_\zeta^\beta(p) = \partial^\beta(p)(\zeta) & = & \displaystyle\sum_{\alpha\in\mathbb{N}^n} p_\alpha^{(\beta)}\,\zeta^\alpha = (\sum_{\alpha\in\mathbb{N}^n} \frac{1}{\alpha!}\,\zeta^\alpha\,\delta^\alpha)(\sum_{\alpha\in\mathbb{N}^n} p_\alpha^{(\beta)}\mathbf{x}^\alpha) \\ & = & \displaystyle(\sum_{\alpha\in\mathbb{N}^n} \frac{1}{\alpha!}\,\zeta^\alpha\,\partial^\alpha)\partial^\beta(p)(\zeta) = \Big(\delta^\beta\,\Delta(\zeta,\delta)\Big)\,(p). \end{array}$$

Ce qui montre que $\delta_\zeta^\beta = \delta^\beta\,\Delta(\zeta,\delta)$ dans $\mathbb{K}[[\delta]]$. □

Notons que

$$\Delta(\delta,\zeta) = \sum_{\alpha\in\mathbb{N}^n} \zeta^\alpha \mathbf{d}^\alpha$$

mais, comme $\mathbf{d}^\alpha\mathbf{d}^\beta = \binom{\alpha+\beta}{\alpha}\mathbf{d}^{\alpha+\beta}$, on a $\mathbf{d}_\zeta^\alpha \neq \mathbf{d}^\alpha \sum_{\alpha\in\mathbb{N}^n}\zeta^\alpha\mathbf{d}^\alpha$, au sens habituel du produit des séries. De ce point de vue, l'utilisation des séries en δ est donc plus naturelle, et à relier avec les transformées de Fourier.

7.1.4. L'orthogonal d'un idéal. —

***Définition* 7.6.** *Pour tout idéal* I *de* R*, on définit le sous-espace vectoriel de* $\widehat{R}$ *suivant :*

$$I^\perp = \{\Lambda \in \widehat{R};\ \forall p \in I,\ \Lambda(p) = 0\}.$$

Pour tout sous-espace vectoriel $\mathcal{D}$ *de* $\widehat{R}$*, on définit le sous-espace vectoriel de* R *suivant :*

$$\mathcal{D}^\perp = \{p \in R;\ \forall \Lambda \in \mathcal{D},\ \Lambda(p) = 0\}.$$

L'espace vectoriel $I^\perp$ est appelé dans la littérature le *système inverse* de I (voir [**Mac16**]).

***Remarque* 7.7.** L'orthogonal d'un idéal I de R n'est pas un idéal de $\mathbb{K}[[\mathbf{d}]]$.

***Exemple* 7.8.** *Dans* $\mathbb{K}[x_1,x_2]$*,* $\mathcal{D} := \langle \mathbf{1}, \delta_1, \delta_2, \delta_1\delta_2\rangle$ *est l'orthogonal de l'idéal* $I = (x_1^2, x_2^2)$*.*

Les éléments de $I^\perp$ peuvent se voir comme des formes linéaires sur $\mathcal{A} = R/I$. La projection $\pi : R \to \mathcal{A}$ induit une application

$$\begin{array}{rcl} \pi_* : \widehat{\mathcal{A}} & \to & I^\perp \\ \Lambda & \mapsto & \Lambda\circ\pi. \end{array}$$

***Proposition* 7.9.** *L'application π_* est un isomorphisme entre $I^\perp$ et $\widehat{\mathcal{A}}$.*

***Exemple* 7.10.** *Dans l'exemple précédent, $\mathbb{K}[x_1, x_2]/I$ a pour base $\{1, x_1, x_2, x_1x_2\}$ et la base duale s'identifie à $\{\mathbf{1}, \delta_1, \delta_2, \delta_1\delta_2\}$.*

Dans la suite, on identifiera de même $I^\perp$ avec $\widehat{\mathcal{A}}$. Le système inverse $I^\perp$ est stable par dérivation. En fait, il y a une correspondance entre les idéaux de R et certains sous-espaces vectoriels de $\mathbb{K}[[\delta_\zeta]]$ stables par dérivation et fermé pour la topologie $(\delta_{1,\zeta}, \ldots, \delta_{n,\zeta})$-adique, que nous rappelons en terme de convergence des suites. Pour cette topologie, une suite $(\Lambda_l)_{l\in\mathbb{N}}$ converge vers Λ ssi pour tout $k \in \mathbb{N}$, il existe $l_0 \in \mathbb{N}$ tel que pour $l \geq l_0$, $\Lambda_l - \Lambda \in (\delta_{1,\zeta}, \ldots, \delta_{n,\zeta})^k$. Voir [**Mal85**].

***Théorème* 7.11.** *Les idéaux de R sont en bijection avec les sous-espaces vectoriels de $\mathbb{K}[[\delta_\zeta]]$ stables par dérivation et fermés pour la topologie $(\delta_{1,\zeta}, \ldots, \delta_{n,\zeta})$-adique.*

Voir [**Ems78**]. Cette bijection consiste à prendre l'orthogonal dans le dual et dans le bidual, c'est-à-dire l'espace lui-même. Pour tout idéal I de R et pour tout sous-espace vectoriel fermé $\mathcal{D}$ de $\widehat{R}$, on a en effet les propriétés

$$I^{\perp\perp} = I,\ \mathcal{D}^{\perp\perp} = \mathcal{D}.$$

Nous donnons quelques propriétés directes des systèmes inverses.

***Proposition* 7.12.** *Soient I et J deux idéaux de R, alors*
- $I \subset J \Leftrightarrow J^\perp \subset I^\perp$
- $(I \cap J)^\perp = I^\perp + J^\perp$
- $(I + J)^\perp = I^\perp \cap J^\perp$.

***Définition* 7.13.** *Nous dirons qu'un sous-espace vectoriel L de $\widehat{R}$ est stable si $\forall \Lambda \in L$,*

$$x_i \cdot \Lambda \in \langle L \rangle, \text{ pour } i = 1, \ldots, n.$$

Nous avons vu que la multiplication d'une forme linéaire par une variable s'interprète comme une dérivation dans l'espace des séries formelles associé. Cette définition nous permet d'énoncer facilement le résultat suivant :

***Lemme* 7.14.** *$\mathcal{D} = \{\Lambda_1, \ldots, \Lambda_D\}$ est stable, si et seulement si, $\mathcal{D}^\perp$ est un idéal.*

Démonstration. Supposons $\mathcal{D}$ stable. Soit $p \in \mathcal{D}^\perp$. Pour tout $i = 1, \ldots, n$, $j = 1, \ldots, D$, on a $\Lambda_j(x_i\, p) = x_i \cdot \Lambda_j(p) = \sum_{k=1}^{D} \lambda_{i,j,k}\Lambda_k(p) = 0$ $(\lambda_{i,j,k} \in \mathbb{K})$. Ce qui montre que l'espace vectoriel $\mathcal{D}^\perp$ est stable par multiplication par les variables x_i. C'est donc un idéal de $\mathbb{K}[\mathbf{x}]$.

Inversement, supposons que $\mathcal{D}^\perp$ soit un idéal. Pour tout $p \in \mathcal{D}^\perp$ et $i = 1, \ldots, n$, $x_i\, p \in \mathcal{D}^\perp$ et donc pour tout $j = 1, \ldots, D$, $\Lambda_j(x_i\, p) = x_i \cdot \Lambda(p) = 0$.

Ceci nous montre que $x_i \cdot \Lambda_j \in \mathcal{D}^{\perp\,\perp} = \langle \mathcal{D} \rangle$ (voir théorème 7.11). □

Par le théorème 7.11, les espaces stables de $\widehat{R}$ sont de la forme $I^\perp$ pour I idéal de R.

Ce qui nous conduit à la définition d'un *système inverse* engendré par des formes linéaires :

***Définition* 7.15.** *Soient $\Lambda_1, \ldots, \Lambda_s \in \mathbb{K}[[\delta_\zeta]]$, on note*

$$\langle\langle \Lambda_1, \ldots, \Lambda_s \rangle\rangle,$$

le système inverse engendré par $\Lambda_1, \ldots, \Lambda_s$. C'est le sous-espace vectoriel de $\mathbb{K}[[\delta_\zeta]]$ engendré par les éléments Λ_i et toutes leurs dérivées.

***Exemple* 7.16.** *Dans $\mathbb{K}[x_1, x_2]$, le système inverse engendré par $\mathbf{d}_2^2\mathbf{d}_1 + \mathbf{d}_2$ est*

$$\langle \mathbf{d}_1\mathbf{d}_2^2 + \mathbf{d}_2, \mathbf{d}_2^2, \mathbf{d}_1\mathbf{d}_2 + \mathbf{1}, \mathbf{d}_1, \mathbf{d}_2, \mathbf{1} \rangle = \langle \mathbf{d}_1\mathbf{d}_2^2 + \mathbf{d}_2, \mathbf{d}_2^2, \mathbf{d}_1\mathbf{d}_2, \mathbf{d}_1, \mathbf{d}_2, \mathbf{1} \rangle.$$

7.1.5. Division d'idéaux. — Certaines propriétés des idéaux, difficiles à décrire ou à calculer dans R, se traduisent particulièrement bien sur les systèmes inverses. La division en est un exemple.

***Proposition* 7.17.** *Pour tout $\Lambda_1, \ldots, \Lambda_s \in \mathbb{K}[[\delta_\zeta]]$, et $p_1, \ldots, p_t \in R$,*

$$\langle\langle \Lambda_1, \ldots, \Lambda_s \rangle\rangle^\perp : (p_1, \ldots, p_t) = \langle\langle p_j \cdot \Lambda_i \rangle\rangle^\perp_{1 \le i \le s, 1 \le j \le t}$$

Démonstration. Comme $\langle\langle \Lambda_1, \ldots, \Lambda_s \rangle\rangle^\perp$ est un idéal de R,

$$\begin{aligned} P \in \langle\langle \Lambda_1, \ldots, \Lambda_s \rangle\rangle^\perp : (p_1, \ldots, p_t) &\Leftrightarrow \forall j,\ p_j\, P \in \langle\langle \Lambda_1, \ldots, \Lambda_s \rangle\rangle^\perp \\ &\Leftrightarrow \forall i, j, \forall Q \in R,\ \Lambda_i(p_j\, P\, Q) = 0 \\ &\Leftrightarrow \forall i, j, \forall Q \in R, p_j \cdot \Lambda_i(P\, Q) = 0 \\ &\Leftrightarrow P \in \langle\langle p_j \cdot \Lambda_i \rangle\rangle^\perp. \end{aligned}$$

□

***Exemple* 7.18.** *Dans $\mathbb{K}[x_1, x_2]$, si $\mathcal{D} = \langle\langle \mathbf{d}_2^2\mathbf{d}_1 + \mathbf{d}_2 \rangle\rangle$ alors $\mathcal{D}^\perp : (x_1, x_2) = \langle\langle \mathbf{d}_2^2, \mathbf{d}_1\mathbf{d}_2 + \mathbf{1} \rangle\rangle^\perp = \langle\langle \mathbf{d}_2^2, \mathbf{d}_1\mathbf{d}_2 \rangle\rangle^\perp = (x_1^2, x_1x_2^2, x_2^3)$.*

7.1.6. Élimination de variables. — La projection ou l'élimination de variables est un deuxième exemple de propriétés qui se traduisent bien sur les systèmes inverses. Soit $r \in \{1, \ldots, n\}$; pour tout idéal I de R, $\sigma_r(I^\perp) = \{\sigma_r(\Lambda) = \Lambda(\mathbf{d}_1, \ldots, \mathbf{d}_r, 0, \ldots, 0); \Lambda \in I^\perp\}$. Pour tout idéal $I \subset R_r$, $I^{\perp_r} = I^\perp \cap \mathbb{K}[[\mathbf{d}_1, \ldots, \mathbf{d}_r]]$, où $I^\perp \subset \mathbb{K}[[\mathbf{d}_1, \ldots, \mathbf{d}_n]]$.

***Proposition* 7.19.** *Pour tout idéal I de R, $(I \cap R_r)^{\perp_r} = \sigma_r(I^\perp)$.*

Démonstration. Comme $R_r^\perp = \langle\langle \mathbf{d}_{r+1}, \ldots, \mathbf{d}_n \rangle\rangle$,

$$\begin{aligned}(I \cap R_r)^{\perp_r} &= (I \cap R_r)^\perp \cap \widehat{R}_r = (I^\perp + R_r^\perp) \cap \widehat{R}_r \\ &= (I^\perp + \langle\langle \mathbf{d}_{r+1}, \ldots, \mathbf{d}_n \rangle\rangle) \cap \widehat{R}_r = \sigma_r(I^\perp).\end{aligned}$$

□

***Exemple* 7.20.** *Dans* $\mathbb{K}[x_1, x_2]$, *si* $\mathcal{D} = \langle\langle \mathbf{d}_2^2 \mathbf{d}_1 + \mathbf{d}_2 \rangle\rangle$ *alors*

$$\mathcal{D}^\perp \cap \mathbb{K}[x_1] = \langle \mathbf{d}_1, \mathbf{1} \rangle^\perp \cap \mathbb{K}[x_1] = (x_1^2).$$

7.1.7. Équations différentielles et système inverse. —

***Proposition* 7.21.** *Soit* $I = (p_1, \ldots, p_s)$ *un idéal de* R *; alors son système inverse*

$$I^\perp = \{\Lambda \in \mathbb{K}[[\delta_\zeta]];\ p_i(\zeta_1 + \partial_{\delta_{1,\zeta}}, \ldots, \zeta_n + \partial_{\delta_{n,\zeta}})(\Lambda) = 0, 1 \leq i \leq s\}.$$

Démonstration. Nous avons vu que si $\Lambda \in \mathbb{K}[[\delta_\zeta]], (x_i - \zeta_i) \cdot \Lambda = \partial_{\delta_{i,\zeta}}(\Lambda)$. Donc, pour tout $P \in R, P \cdot \Lambda = P(\zeta_1 + \partial_{\delta_{1,\zeta}}, \ldots, \zeta_n + \partial_{\delta_{n,\zeta}})(\Lambda)$. Ceci montre que $\Lambda \in I^\perp$ si et seulement si $\forall q \in R$, $\forall i = 1, \ldots, s$,

$$\Lambda(p_i\, q) = p_i \cdot \Lambda(q) = p_i(\zeta_1 + \partial_{\delta_{1,\zeta}}, \ldots, \zeta_n + \partial_{\delta_{n,\zeta}})(\Lambda)(q) = 0.$$

□

La proposition permet de voir la résolution de systèmes d'équations différentielles à coefficients constants et la réduction modulo un idéal de R comme le même problème. Voir [**Ped96**] à propos de cette remarque, que nous illustrons par un exemple :

***Exemple* 7.22.** *Considérons le système différentiel*

$$\begin{cases} \frac{\partial^2}{\partial_t^2}\phi - \frac{\partial^2}{\partial_s^2}\phi = 0 \\ \frac{\partial^2}{\partial_t \partial_s}\phi - \phi = 0. \end{cases} \tag{7.1}$$

Nous cherchons les solutions dans l'espace des séries formelles. Dans le contexte précédent, $\phi \in \mathbb{K}[[\delta_1, \delta_2]]$ *est donc un élément du dual de* $R = \mathbb{K}[x_1, x_2]$ *où* $t = \delta_1$ *et* $s = \delta_2$ *sont les variables duales de* x_1, x_2*. Le système précédent se traduit par*

$$\begin{cases} f_1 \cdot \phi = 0 \\ f_2 \cdot \phi = 0 \end{cases}$$

où $f_1 = x_1^2 - x_2^2$ *et* $f_2 = x_1 x_2 - 1$*. La série formelle* ϕ *est dans l'orthogonal de* $I = (f_1, f_2)$*, ou encore dans le dual de* $\mathcal{A} = \mathbb{K}[x_1, x_2]/(f_1, f_2)$*. Ce quotient est de dimension* 4 *(par le théorème de Bézout, car il n'y a pas de zéro à l'infini), et les zéros sont*

$$\zeta_1 = (1, 1),\ \zeta_2 = (-1, -1),\ \zeta_3 = (\mathbf{i}, -\mathbf{i}),\ \zeta_4 = (-\mathbf{i}, \mathbf{i}).$$

Le dual est donc l'espace vectoriel engendré par $\mathbf{1}_{\zeta_1},\ \mathbf{1}_{\zeta_2},\ \mathbf{1}_{\zeta_3},\ \mathbf{1}_{\zeta_4}$, *c'est-à-dire par*

$$\exp(\delta_1+\delta_2), \exp(-\delta_1-\delta_2), \exp(\mathbf{i}\delta_1-\mathbf{i}\delta_2), \exp(-\mathbf{i}\delta_1+\mathbf{i}\delta_2).$$

En revenant à notre problème initial (c'est-à-dire en remplaçant δ_1 *par* t *et* δ_2 *par* s*), nous voyons que les solutions de (7.1) sont de la forme*

$$\phi = \lambda_1\, ch(s+t) + \lambda_2\, sh(s+t) + \lambda_3\, cos(s-t) + \lambda_4\, sin(s-t),$$

7.1.8. Passage du système inverse au quotient. — La construction d'une base de $I^\perp$ peut se faire facilement si on sait réduire tout polynôme en une forme normale modulo I. Les éléments du système inverse de I ont la même valeur sur tous les éléments qui se réduisent à un même terme. Soient I un idéal de R et $(\mathbf{x}^\alpha)_{\alpha\in E}$ une base de $\mathcal{A} = R/I$. Alors pour tout monôme $\mathbf{x}^\beta$, il existe des scalaires uniques $(\lambda_{\alpha,\beta})$, tels que

$$\mathbf{x}^\beta - \sum_{\alpha\in E} \lambda_{\alpha,\beta}\, \mathbf{x}^\alpha \in I. \tag{7.2}$$

***Proposition* 7.23.** *La famille*

$$(\mathbf{d}^\alpha + \sum_{\beta\in\mathbb{N}^n\setminus E} \lambda_{\alpha,\beta}\, \mathbf{d}^\beta)_{\alpha\in E}$$

forme une base du système inverse de I.

Démonstration. Soit $(\Lambda_\alpha) \subset \widehat{\mathcal{A}}$ (que l'on identifie avec $I^\perp$) la base duale de $(\mathbf{x}^\alpha) \subset \mathcal{A}$. Les éléments Λ_α s'écrivent sous la forme

$$\Lambda_\alpha = \sum_{\beta\in\mathbb{N}^n} \mu_{\beta,\alpha}\, \mathbf{d}^\beta, \mu_{\alpha,\beta} \in \mathbb{K}.$$

D'après les relations (7.2), pour $\beta \notin E$ on a

$$\mu_{\alpha,\beta} = \Lambda_\alpha(\mathbf{x}^\beta) = \sum_{\alpha'} \lambda_{\alpha',\beta}\, \Lambda_\alpha(\mathbf{x}^{\alpha'}) = \lambda_{\alpha,\beta}.$$

Par ailleurs, pour $\beta \in E$, on a $\mu_{\alpha,\beta} = \Lambda_\beta(\mathbf{x}^\alpha) = 1$ si $\beta = \alpha$ et 0 sinon. □

***Exemple* 7.24.** *Considérons les polynômes* $f_1 = x_1^2 - 1, f_2 = x_2^2 - 2\,x_1 \in \mathbb{K}[x_1, x_2]$. *Une base de* $\mathcal{A} = \mathbb{K}[x_1, x_2]/(f_1, f_2)$ *est* $\{1, x_1, x_2, x_1, x_2\}$. *Si nous construisons la matrice*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & \cdots \\ 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & \cdots \end{pmatrix}$$

correspondant aux coefficients des formes normales de

$$1, x_1, x_2, x_1\,x_2, x_1^2, x_2^2, x_1^3, x_1^2x_2, x_1x_2^2, x_2^3, \ldots$$

Les lignes de cette matrice correspondent respectivement aux coefficients dans $\Lambda_1, \Lambda_{x_1}, \Lambda_{x_2}, \Lambda_{x_1,x_2} \in \mathbb{K}[[\mathbf{d}_1, \mathbf{d}_2]]$ *des termes*

$$\mathbf{1}, \mathbf{d}_1, \mathbf{d}_2, \mathbf{d}_1\,\mathbf{d}_2, \mathbf{d}_1^2, \mathbf{d}_2^2, \mathbf{d}_1^3, \mathbf{d}_1^2\mathbf{d}_2, \mathbf{d}_1\mathbf{d}_2^2, \mathbf{d}_2^3, \ldots$$

Ceci nous conduit à une méthode effective pour calculer les premiers termes du développement de Λ_α, si nous savons calculer les relations (7.2). Ceci est possible si nous avons une méthode de normalisation sur la base $(\mathbf{x}^\alpha)_{\alpha\in E}$ modulo I. C'est le cas par exemple quand on connaît une base de Gröbner $(g_1, \ldots, g_s)$ de l'idéal I, pour un ordre monomial $<$. La base $(\mathbf{x}^\alpha)_{\alpha\in E}$ sera alors l'ensemble des monômes en dehors de l'initial $\mathtt{m}_<(I)$ de I. Nous appelerons fonction de normalisation N sur $(\mathbf{x}^\alpha)_{\alpha\in E}$ modulo I, la projection de R sur $\langle \mathbf{x}^\alpha \rangle_{\alpha\in E}$ parallèlement à I.

***Algorithme* 7.25.** BASE DUALE DE LA BASE $(\mathbf{x}^\alpha)_{\alpha\in E}$ DE R/I.

ENTRÉE : `Une fonction de normalisation` N `sur` $(\mathbf{x}^\alpha)_{\alpha\in E}$ `modulo` I.
`Pour tout` $\mathbf{x}^\beta$ `de degré` $\leq k$ `avec` $\beta \notin E$,
  `Calculer` $N(\mathbf{x}^\beta) = \sum_{\alpha\in E} \lambda_{\alpha,\beta}\mathbf{x}^\beta$;
  `Pour` $\alpha \in E$, $\Lambda_\alpha := \Lambda_\alpha + \lambda_{\alpha,\beta}\,\mathbf{d}^\beta$;
SORTIE : `Les termes de la base duale` Λ_α `jusqu'au degré` k.

Nous venons de voir comment passer d'une base du quotient à sa base duale. Cette construction peut se reformuler à l'aide de l'objet suivant :

$$\Delta = \sum_{\alpha\in\mathbb{N}^n} \mathbf{x}^\alpha \otimes \mathbf{d}^\alpha$$

l'élément diagonal de $\mathbb{K}[[\mathbf{x}, \mathbf{d}]]$. Pour $p \in R$, on définit $\Delta(p) = \sum_{\alpha\in\mathbb{N}^n} \mathbf{x}^\alpha \mathbf{d}^\alpha(p)$, et pour $\lambda \in \widehat{R}, \lambda(\Delta) = \sum_{\alpha\in\mathbb{N}^n} \lambda(\mathbf{x}^\alpha)\mathbf{d}^\alpha$. On vérifie que

$$\Delta(p) = p,\ \lambda(\Delta) = \lambda.$$

Nous nous plaçons dans le cas où $\mathcal{A}$ *est un* $\mathbb{K}$*-espace vectoriel de dimension finie.*

***Proposition* 7.26.** *Les propriétés suivantes sont équivalentes*

1. *Il existe une décomposition de* Δ *sous la forme*

$$\Delta = \sum_{i=1}^{\infty} a_i \otimes b_i$$

   où les familles (a_i) *et* (b_i) *sont linéairement indépendantes sur* $\mathbb{K}$ *avec*
   - $a_j \in I$ *pour* $j > \mu$,
   - $b_i \in I^\perp$ *pour* $1 \leq i \leq \mu$.
2. $(a_i)_{1\leq i\leq\mu}$ *est une base de* $\mathcal{A}$.
3. $(b_i)_{1\leq i\leq\mu}$ *est une base de* $I^\perp$.

Si ces points sont satisfaits, alors $(a_i)_{1\le i\le\mu}$ *et* $(b_i)_{1\le i\le\mu}$ *sont des bases duales.*

Démonstration. Supposons que Δ se décompose suivant *1.* Puisque (a_i) engendre $\mathbb{K}[\mathbf{x}]$ (comme $\mathbb{K}$-espace vectoriel), $(a_i)_{1\le i\le\mu}$ engendre $\mathcal{A}$.

Nous avons de plus $b_i(\Delta) = b_i = \sum_{j=1}^{\mu} b_i(a_j)\, b_j$; ceci implique

$$b_i(a_j) = \delta_{i,j} \text{ pour } 1 \le i, j \le \mu, \tag{7.3}$$

où $\delta_{i,j}$ est le symbole de Kronecker. Par conséquent, $(a_i)_{1\le i\le\mu}$ est libre dans $\mathcal{A}$. En effet, si $\sum_{l=1}^{\mu} \lambda_l\, a_l \in I$, alors $b_i(\sum_l \lambda_l\, a_l) = 0$ et $\lambda_l = 0$ pour $1 \le l \le \mu$. Ainsi $(a_i)_{1\le i\le\mu}$ est une base de $\mathcal{A}$. La relation (7.3) montre que $(b_i)_{1\le i\le\mu}$ est la base duale de $(a_i)_{1\le i\le\mu}$ et les points 2 et 3 sont vérifiés.

Supposons maintenant que le point 2 soit vérifié. Alors il existe une famille libre $(a_j)_{j>\mu} \subset I$ telle que l'espace vectoriel engendré par $(a_1, \ldots, a_\mu, a_{\mu+1}, \ldots)$ soit une base de $\mathbb{K}[\mathbf{x}]$. Ceci permet de réécrire Δ sous la forme

$$\Delta = \sum_{i=1}^{\mu} a_i \otimes b'_i + \sum_{j>\mu} a_j \otimes b'_j,$$

avec les (b'_j) linéairement indépendants. Soit $(b_i)_{1\le i\le\mu} \subset I^\perp$ la base duale de $(a_i)_{1\le i\le\mu}$. On a alors

$$b_i(\Delta) = b_i = \sum_{j=1}^{\mu} b_i(a_j) b'_j = b'_i\ , \quad 1 \le i \le \mu$$

ce qui montre le point 1.

Si le point 3 est vérifié, alors on choisit pour (a_i) la base duale de (b_i) et on utilise le 2. □

Cette propriété peut être utilisée dans les deux sens. Si nous savons réduire tout monôme à une forme normale (par exemple, en utilisant une base de Gröbner) alors nous pouvons calculer une base du système inverse (au moins en tronquant à un certain degré). Inversement, si nous connaissons le système inverse alors nous pouvons construire les générateurs de l'idéal. Nous illustrons ceci sur deux exemples très simples, où les éléments du système inverse sont des polynômes en $\mathbf{d}$.

***Exemple* 7.27.** *Nous considérons l'idéal* I *engendré par*

$$p_1 := y - x^2,\ p_2 := y^2 - x^3,\ p_3 := x^4.$$

Pour construire $I^\perp$*, nous utilisons les relations* $x\,y \equiv x^3 \equiv y^2 \equiv x^4 \equiv 0$ *modulo* I *et* $x^2 = y - p_1$*. On réécrit* Δ *sous la forme*

$$\begin{aligned}
\Delta &= \mathbf{d}^0 + x\,\mathbf{d}_1 + y\,\mathbf{d}_2 + x^2\,\mathbf{d}_1^2 + \cdots \\
&= \mathbf{d}^0 + x\,\mathbf{d}_1 + y\,\mathbf{d}_2 + (y - p_1)\,\mathbf{d}_1^2 + \cdots \\
&= \mathbf{d}^0 + x\,\mathbf{d}_1 + y\,(\mathbf{d}_2 + \mathbf{d}_1^2) + \cdots
\end{aligned}$$

les points de suspension $\cdots$ désignant des éléments de $I \otimes \widehat{R}$. Les produits tensoriels sont implicites dans cette notation. Donc $I^\perp = \langle \mathbf{d}_2 + \mathbf{d}_1^2, \mathbf{d}_1, \mathbf{d}^0 \rangle = \langle\langle \mathbf{d}_2 + \mathbf{d}_1^2 \rangle\rangle$.

***Exemple* 7.28.** *Nous considérons le système inverse*

$$\langle\langle \mathbf{d}_1^2 + \mathbf{d}_2^2 + \mathbf{d}_1\mathbf{d}_2 \rangle\rangle$$

qui est engendré (comme $\mathbb{K}$-espace vectoriel) par les éléments $\Lambda_2 = \mathbf{d}_1^2 + \mathbf{d}_2^2 + \mathbf{d}_1\mathbf{d}_2, \Lambda_1 = \mathbf{d}_1 + \mathbf{d}_2, \Lambda_0 = \mathbf{d}^0$, et nous voulons construire l'idéal I. On réécrit Δ sous la forme

$$\begin{aligned}
\Delta &= \mathbf{d}^0 + x\,\mathbf{d}_1 + y\,\mathbf{d}_2 + x^2\,\mathbf{d}_1^2 + x\,y\,\mathbf{d}_1\,\mathbf{d}_2 + y^2\,\mathbf{d}_2^2 + \cdots \\
&= \Lambda_0 + x\,(\Lambda_1 - \mathbf{d}_2) + y\,\mathbf{d}_2 + x^2\,(\Lambda_2 - \mathbf{d}_2^2 - \mathbf{d}_1\,\mathbf{d}_2) + x\,y\,\mathbf{d}_1\,\mathbf{d}_2 + y^2\,\mathbf{d}_2^2 + \cdots \\
&= \Lambda_0 + x\,\Lambda_1 + x^2\,\Lambda_2 + (y - x)\,\mathbf{d}_2 + (x\,y - x^2)\,\mathbf{d}_1\,\mathbf{d}_2 + (y^2 - x^2)\,\mathbf{d}_2^2 + \cdots
\end{aligned}$$

On voit donc que

$$\langle\langle \mathbf{d}_1^2 + \mathbf{d}_2^2 + \mathbf{d}_1\mathbf{d}_2 \rangle\rangle^\perp = (x - y) + (x, y)^3,$$

et que $(1, x, x^2)$ est une base du quotient $\mathcal{A}$.

Dans le cas où $\mathcal{A}$ est un espace vectoriel de dimension finie, la structure multiplicative du quotient peut se retrouver directement, comme le montre la proposition suivante. Soit $(\hat{b}_1, \ldots, \hat{b}_\mu)$ une base de l'espace vectoriel $I^\perp$. Pour tout $k \in \{1, \ldots, n\}$,

$$\partial_{\delta_k}(\hat{b}_i) = \sum_{j=1}^{\mu} \lambda_{i,j}^k \hat{b}_j \quad , \quad \lambda_{i,j}^k \in \mathbb{K}.$$

Notons M_k la matrice $(\lambda_{i,j}^k)_{1 \le i,j \le \mu}$.

***Proposition* 7.29.** *Les matrices $M_k, 1 \le k \le n$, sont les matrices de multiplication par x_k dans $\mathcal{A}$ dans la base duale de $(b_i)_{1 \le i \le \mu}$.*

Démonstration. Soit $(b_1, \ldots, b_\mu)$ la base duale de $(\hat{b}_1, \ldots, \hat{b}_\mu)$ dans $\mathcal{A}$. Le coefficient d'indices i, j de la matrice de multiplication par x_k dans $\mathcal{A}$ dans la base (b_j) est donné par

$$\begin{aligned}
\hat{b}_i(x_k\,b_j) &= (x_k \cdot \widehat{b_i})(b_j) \\
&= \partial_{\delta_k}(\hat{b}_i)(b_j) = \sum_{l=1}^{\mu} \lambda_{i,l}^k \hat{b}_l(b_j) = \lambda_{i,j}^k.
\end{aligned}$$

□

7.2. Système inverse d'un point isolé

Nous nous plaçons dans le cas où l'idéal I définit un point isolé $\zeta \in \mathbb{K}^n$, et nous notons $\mathfrak{m}_\zeta$ l'idéal maximal définissant ζ. Dans cette section, nous allons décrire une méthode permettant de calculer la structure locale de I en ζ.

7.2.1. Points isolés. — Caractérisons dans un premier temps, les systèmes inverses de points multiples.

***Proposition* 7.30.** *Supposons que I soit $\mathfrak{m}_\zeta$-primaire ; alors $I^\perp \subset \mathbb{K}[\delta_\zeta]$.*

Démonstration. Puisqu'il existe un entier N tel que $\mathfrak{m}_\zeta^N \subset I \subset \mathfrak{m}_\zeta$, $(\mathbf{x}-\zeta)^\alpha \in I$ dès que $|\alpha| = a_1 + \cdots + a_n \geq N$. Soit $\Lambda \in I^\perp$, alors

$$\Lambda = \sum_{\alpha \in \mathbb{N}^n : |\alpha| < N} \frac{1}{\alpha!} \Lambda((\mathbf{x}-\zeta)^\alpha)\, \delta_\zeta^\alpha.$$

□

Dans ce cas, les éléments du système inverse de I sont des polynômes en δ_ζ. De plus, $\mathcal{A} = R/I$ est de dimension finie μ sur $\mathbb{K}$ (où μ est la multiplicité de la racine ζ), par suite $I^\perp$ est un espace vectoriel de dimension μ.

Ceci établit *une bijection entre les idéaux $\mathfrak{m}_\zeta$-primaires et les sous-espaces vectoriels de $\mathbb{K}[\delta_\zeta]$, stables par dérivation et de dimension finie* (voir [**Ems78**], [**Mac16**][p. 65], [**Grö70**]).

7.2.2. La composante $\mathfrak{m}_\zeta$-primaire. — Dans la pratique, il est rare de traiter directement un idéal $\mathfrak{m}_\zeta$-primaire ; on a souvent affaire à des idéaux dont une composante est $\mathfrak{m}_\zeta$-primaire. Nous allons voir comment on peut isoler cette composante, c'est-à-dire oublier le reste de la variété.

***Théorème* 7.31.** *Soit I un idéal de R et Q_ζ sa composante $\mathfrak{m}_\zeta$-primaire que l'on suppose isolée. Alors*

$$(I^\perp \cap \mathbb{K}[\delta_\zeta])^\perp = Q_\zeta.$$

Démonstration. Notons $\mathcal{D}_\zeta = I^\perp \cap \mathbb{K}[\delta_\zeta]$; nous allons montrer que $\mathcal{D}_\zeta = Q_\zeta^\perp$. On a $Q_\zeta^\perp \subset I^\perp$ (car $I \subset Q_\zeta$) et $Q_\zeta^\perp \subset \mathbb{K}[\delta_\zeta]$ (d'après la proposition (7.30)), par suite, $Q_\zeta^\perp \subset I^\perp \cap \mathbb{K}[\delta_\zeta]$. Pour montrer l'inclusion inverse, nous utiliserons les deux propriétés suivantes :

- La composante $\mathfrak{m}_\zeta$-primaire Q_ζ de I est l'ensemble des polynômes f de R tels qu'il existe $g \in R$ avec $f\,g \in I$ et $g(\zeta) \neq 0$ (voir [**AM69**]).
- Pour tout $\Lambda \in \mathbb{K}[\delta_\zeta]$ et tout $g \in R$,

$$\begin{aligned} (g \cdot \Lambda)(f) &= g(\zeta_1 + \partial_{\delta_{1,\zeta}}, \ldots, \zeta_n + \partial_{\partial_{n,\zeta}})(\Lambda)(f) \qquad (7.4)\\ &= g(\zeta)\Lambda(f) + (g - g(\zeta))(\zeta_1 + \partial_{\delta_{1,\zeta}}, \ldots, \zeta_n + \partial_{\delta_{n,\zeta}})(\Lambda)(f). \end{aligned}$$

Montrons par récurrence sur le degré de Λ (en $\delta_\zeta = (\delta_{1,\zeta}, \ldots, \delta_{n,\zeta})$) que $\mathcal{D}_\zeta \subset Q_\zeta^\perp$.

Si $\Lambda \in \mathcal{D}_\zeta$, est de degré 0, alors Λ est, à un scalaire près, l'évaluation en ζ. Pour tout $f \in Q_\zeta,\ g \in R$ tels que $g(\zeta) \neq 0$ et $f\,g \in I$, $\Lambda(f\,g) = 0 = f(\zeta)g(\zeta)$, donc $\Lambda(f) = f(\zeta) = 0$, et $\Lambda \in Q_\zeta^\perp$.

Supposons maintenant que tous les éléments de $\mathcal{D}_\zeta$ de degré $< d$ sont dans $Q_\zeta^\perp$. Soit $\Lambda \in \mathcal{D}_\zeta$ de degré d; d'après la formule (7.4), pour tout $f \in Q_\zeta$, $g \in R$ tels que $g(\zeta) \neq 0$ et $fg \in I$,

$$\begin{aligned}\Lambda(f\,g) = \quad 0 = \quad & g(\zeta)\Lambda(f) + (g - g(\zeta))(\zeta_1 + \partial_{\delta_{1,\zeta}}, \ldots, \zeta_n + \partial_{\delta_{n,\zeta}})(\Lambda)(f) \\ = \quad & g(\zeta)\Lambda(f) + \rho(f),\end{aligned}$$

$\rho = (g - g(\zeta))(\zeta_1 + \partial_{\delta_{1,\zeta}}, \ldots, \zeta_n + \partial_{\delta_{n,\zeta}})(\Lambda)$ est de degré $< d$ en δ_ζ et $\rho \in \mathcal{D}_\zeta$ (car $\mathcal{D}_\zeta$ est stable par dérivation). Par hypothèse de récurrence, $\rho(f) = 0$. Il en découle que $\Lambda(f) = 0$, et $\Lambda \in Q_\zeta^\perp$. □

Soit $N \in \mathbb{N}$ tel que $\mathfrak{m}_\zeta^N \subset Q_\zeta$; alors le degré des éléments de $\mathcal{D}_\zeta$ est au plus N.

***Définition* 7.32.** *On appelle l'indice de nilpotence de Q_ζ l'entier N_ζ égal au maximum des degrés des éléments de $\mathcal{D}_\zeta$.*

On vérifie facilement que N_ζ est le plus petit entier N tel que

$$\mathfrak{m}_\zeta^N \not\subset Q_\zeta.$$

En effet, pour tout $\Lambda \in \mathcal{D}_\zeta$ de degré N_ζ, il existe un monôme $m = (\mathbf{x} - \zeta)^\alpha$ de degré N_ζ tel que $\Lambda(m) \neq 0$, donc $\mathfrak{m}_\zeta^{N_\zeta} \not\subset Q_\zeta$. Par contre, pour tout monôme $m = (\mathbf{x} - \zeta)^\alpha$ tel que $|\alpha| > N_\zeta$ et tout $\Lambda \in \mathcal{D}_\zeta$, $\Lambda(m) = 0$, donc $(\mathbf{x} - \zeta)^\alpha \in Q_\zeta$, ce qui implique que $\mathfrak{m}_\zeta^{N_\zeta+1} \subset Q_\zeta$.

***Théorème* 7.33.** *Soient $I = (p_1, \ldots, p_s)$ un idéal de R ayant une composante isolée Q_0 en $\mathbf{0}$, et $q_1, \ldots, q_s$ des polynômes homogènes de degré $> N_0 + 1$. Supposons que*

$$\tilde{I} = (p_1 + q_1, \ldots, p_s + q_s)$$

soit zéro-dimensionnel. Alors $\tilde{I}$ a pour composante $\mathfrak{m}_0$-primaire isolée Q_0.

Démonstration. Notons $\tilde{p}_i = p_i + q_i, 1 \leq i \leq s$. Un élément $\Lambda \in \mathbb{K}[\delta_0]$ est dans $I^\perp$ (resp. $\tilde{I}^\perp$) ssi pour tout $\alpha \in \mathbb{N}^n$, $\Lambda(\mathbf{x}^\alpha\, p_i) = 0$ (resp. $\Lambda(\mathbf{x}^\alpha\, \tilde{p}_i) = 0), 1 \leq i \leq s$. Or si le degré de Λ est $\leq N_0 + 1$,

$$\Lambda(\mathbf{x}^\alpha\, \tilde{p}_i) = \Lambda(\mathbf{x}^\alpha\, p_i).$$

Donc $I^\perp$ et $\tilde{I}^\perp$ coïncident jusqu'au degré $N_0 + 1$. Par conséquent, il n'existe pas d'élément de degré exactement $N_0 + 1$ dans $\tilde{I}^\perp$ (car N_0 est l'indice de

nilpotence de Q_0), et n'a donc pas d'élément de degré $> N_0$ (car $\tilde{I}^\perp$ est stable par dérivation). Il en résulte que

$$\tilde{I}^\perp \cap \mathbb{K}[\delta_0] = I^\perp \cap \mathbb{K}[\delta_0].$$

Comme les zéros de $\tilde{I}$ sont isolés (car $Z(\tilde{I})$ est de dimension 0), il découle du théorème 7.31 que Q_0 est aussi la composante primaire de $\tilde{I}$ à l'origine. □
La composante primaire Q_0 en $\mathbf{0}$ reste inchangée par déformation en degré suffisamment élevé. Ceci est vrai par translation en tout autre point ζ de $\mathbb{K}^n$.

***Théorème* 7.34.** *Soit I un idéal de R définissant des points isolés $\zeta_1, \ldots, \zeta_s$; alors*

$$I^\perp = Q_1^\perp \oplus \cdots \oplus Q_s^\perp,$$

où Q_i est la composante $\mathfrak{m}_{\zeta_i}$-primaire. De plus, pour tout élément Λ de $I^\perp$, il existe des polynômes en $\delta_1, \ldots, \delta_n$ uniques $\Lambda_1, \ldots, \Lambda_n$, tels que

$$\Lambda = \sum_{i=1}^{s} \Lambda_i(\delta)\, \Delta(\zeta_i, \delta). \tag{7.5}$$

Démonstration. Comme $I = Q_1 \cap \cdots \cap Q_s$, $I^\perp = Q_1^\perp + \cdots + Q_s^\perp$. De plus, pour $j_1, \ldots, j_p \in \{1, \ldots, n\}$ et $i \neq j_1, \ldots, j_p$, $Q_i + (Q_{j_1} \cap \cdots \cap Q_{j_p}) = R$, donc $Q_i^\perp \cap (Q_{j_1}^\perp + \cdots + Q_{j_p}^\perp) = R^\perp = \{0\}$ et la somme ci-dessus est directe. Un élément de $I^\perp$ est donc une somme de polynômes de dérivations aux points $\zeta_i, 1 \leq i \leq s$. En utilisant l'isomorphisme (7.5), on obtient la décomposition (7.5). □

7.2.3. L'anneau local par intégration. — Soit I un idéal de R et $\mathcal{D} = I^\perp \cap \mathbb{K}[\delta]$ le système inverse de la composante primaire isolée au point $\zeta = 0$. Notons $\mathbb{K}[\delta]_d$ l'ensemble des polynômes en δ de degré au plus d et $\mathcal{D}_d = \mathcal{D} \cap \mathbb{K}[\delta]_d$. Nous allons voir comment on peut construire $\mathcal{D}_d$ à partir de $\mathcal{D}_{d-1}$. Ainsi si les éléments de I s'annulent en 0, $\mathcal{D}_0$ est engendré par δ^0 (δ^0 est la forme linéaire telle que $\delta^0(p) = p(0)$) et il sera alors possible de construire tous les $\mathcal{D}_j$ par récurrence.

Notons pour $p \in \mathbb{K}[\delta]$, $p_{|\delta_i=0} = p(\delta_1, \ldots, \delta_{i-1}, 0, \delta_{i+1}, \ldots, \delta_n)$.

***Définition* 7.35.** *On appelle i-primitive de $p \in \mathbb{K}[\delta]$ (sans terme constant), le polynôme q, noté $\int_i p$, tel que $\partial_{\delta_i} q = p$ et $q_{|\delta_i=0} = 0$.*

Les éléments de $\mathcal{D}_{d-1}$ sont les dérivées des éléments de $\mathcal{D}_d$; donc pour obtenir les éléments de $\mathcal{D}_d$, l'idée est d'intégrer les éléments de $\mathcal{D}_{d-1}$. La construction de $\mathcal{D}_d$ à partir de $\mathcal{D}_{d-1}$ est basée sur le théorème suivant.

***Théorème* 7.36.** *Supposons que l'idéal I soit engendré par $p_1, \ldots, p_m$ et $d > 1$. Soit $(b_1, \ldots, b_s)$ une base de $\mathcal{D}_{d-1}$. Les éléments de $\mathcal{D}_d$ sans terme constant sont les Λ de la forme*

$$\begin{aligned}\Lambda &= \sum_{j=1}^{s} \lambda_j^1 \int_1 b_j|_{\delta_2=0,\ldots,\delta_n=0} \\ &\quad + \sum_{j=1}^{s} \lambda_j^2 \int_2 b_j|_{\delta_3=0,\ldots,\delta_n=0} + \cdots + \sum_{j=1}^{s} \lambda_j^n \int_n b_j \quad , \quad \lambda_j^k \in \mathbb{K} \ ,\end{aligned} \tag{7.6}$$

tels que

1. $\sum_{j=1}^{s} \lambda_j^k \partial_{\delta_l} b_j - \sum_{j=1}^{s} \lambda_j^l \partial_{\delta_k} b_j = 0$ *pour* $1 \le k < l \le n$,
2. $\Lambda(p_i) = 0$ *pour* $1 \le i \le m$.

Démonstration. Soit $\Lambda \in \mathcal{D}_d$ sans terme constant. Il se décompose de manière unique en

$$\Lambda = \Lambda_1(\delta_1, \ldots, \delta_n) + \Lambda_2(\delta_2, \ldots, \delta_n) + \cdots + \Lambda_n(\delta_n),$$

avec tous les monômes de $\Lambda_i \in \mathbb{K}[\delta_i, \ldots, \delta_n] \backslash \mathbb{K}[\delta_{i+1}, \ldots, \delta_n]$. Alors $\int_i \partial_{\delta_i}(\Lambda_i) = \Lambda_i, 1 \le i \le n$.

Comme $\partial_{\delta_1}(\Lambda) = \partial_{\delta_1}(\Lambda_1) \in \mathcal{D}_{d-1} = \langle b_1, \ldots, b_s \rangle$, il existe des scalaires $\lambda_j^1 \in \mathbb{K}$ tels que

$$\Lambda_1 = \int_1 \partial_{\delta_1}(\Lambda_1) = \sum_{j=1}^{s} \lambda_j^1 \int_1 b_j.$$

Considérons maintenant $\partial_{\delta_2}(\Lambda) = \partial_{\delta_2}(\Lambda_1) + \partial_{\delta_2}(\Lambda_2)$ qui est dans $\mathcal{D}_{d-1}$. Il existe alors $\lambda_j^2 \in \mathbb{K}, 1 \le j \le s$, tels que

$$\begin{aligned}\Lambda_2 = \int_2 \partial_{\delta_2}(\Lambda_2) &= \sum_{j=1}^{s} \lambda_j^2 \int_2 b_j - \int_2 \partial_{\delta_2}(\Lambda_1) \\ &= \sum_{j=1}^{s} \lambda_j^2 \int_2 b_j - (\Lambda_1 - \Lambda_1|_{\delta_2=0}),\end{aligned}$$

car $\int_2 \partial_{\delta_2}(\Lambda_1)$ est la partie de Λ_1 qui *dépend* de δ_2. Par suite

$$\Lambda_1 + \Lambda_2 = \sum_{j=1}^{s} \lambda_j^1 \int_1 b_j|_{\delta_2=0} + \sum_{j=1}^{s} \lambda_j^2 \int_2 b_j.$$

Posons $\sigma_2 = \Lambda_1 + \Lambda_2$. Le même calcul appliqué à $\partial_{\delta_3}(\Lambda)$ donne

$$\Lambda_3 = \sum_{j=1}^{s} \lambda_j^3 \int_3 b_j - (\sigma_2 - \sigma_2|_{\delta_3=0})$$

et

$$\begin{aligned}\Lambda_1+\Lambda_2+\Lambda_3 &= \sum_{j=1}^{s}\lambda_j^1\int_1 b_j|_{\delta_2=0,\delta_3=0}\\ &\quad+\sum_{j=1}^{s}\lambda_j^2\int_2 b_j|_{\delta_3=0}+\sum_{j=1}^{s}\lambda_j^3\int_3 b_j.\end{aligned}$$

Par récurrence, on obtient la formule (7.6) et pour tout $k,l\in\{1,\ldots,n\}$, les relations

$$\sigma_k=\Lambda_1+\cdots+\Lambda_k=\sum_{j=1}^{s}\lambda_j^1\int_1 b_j|_{\delta_2=0,\ldots,\delta_k=0}$$

$$+\sum_{j=1}^{s}\lambda_j^2\int_2 b_j|_{\delta_3=0,\ldots,\delta_k=0}+\cdots+\sum_{j=1}^{s}\lambda_j^k\int_k b_j \tag{7.7}$$

et

$$\Lambda_l=\sum_{j=1}^{s}\lambda_j^l\int_l b_j-(\sigma_{l-1}-\sigma_{l-1}|_{\delta_l=0}). \tag{7.8}$$

Le point 2 est une conséquence directe de $\Lambda\in I^\perp$. Montrons maintenant que le point 1 est vérifié. Nous utilisons, $\partial_{\delta_k}\Lambda_l=0$ pour $k<l$. D'après (7.8), $\partial_{\delta_k}\Lambda_l=0$ entraîne

$$\sum_{j=1}^{s}\lambda_j^l\int_l\partial_{\delta_k}b_j=\partial_{\delta_k}(\sigma_{l-1}-\sigma_{l-1}|_{\delta_l=0}).$$

En dérivant l'égalité précédente par rapport à δ_l, et en utilisant $\partial_{\delta_k}(\sigma_{l-1})=\partial_{\delta_k}(\sigma_k)$ (pour $k<l$), $\partial_{\delta_k}(\sigma_k)=\sum_{j=1}^{s}\lambda_j^k b_j$ (d'après (7.7)), on obtient

$$\sum_{j=1}^{s}\lambda_j^l\partial_{\delta_k}b_j-\sum_{j=1}^{s}\lambda_j^k\partial_{\delta_l}b_j=0.$$

Réciproquement, supposons que Λ soit de la forme (7.6), que les conditions 1, 2 soient satisfaites et montrons que $\Lambda\in\mathcal{D}_d$. Cet élément se décompose en $\Lambda=\Lambda_1+\cdots+\Lambda_n$ avec $\Lambda_k=\sum_{j=1}^{s}\lambda_j^k\int_k b_j-(\sigma_{k-1}-\sigma_{k-1}|_{\delta_k=0})$ et $\sigma_k=\Lambda_1+\cdots+\Lambda_k, 1\le k\le n$ (avec $\sigma_0=0$). Nous avons la relation (7.7) par récurrence. Puisque Λ vérifie 1, d'après ce qui précède, $\partial_{\delta_k}(\Lambda_l)=0$ pour $k<l$ et $\Lambda_l\in\mathbb{K}[\delta_l,\ldots,\delta_n]$. Par construction, Λ_l n'a pas de terme constant et appartient donc à $\mathbb{K}[\delta_l,\ldots,\delta_n]-\mathbb{K}[\delta_{l+1},\ldots,\delta_n]$.

La formule (7.7) implique

$$\partial_{\delta_k}\Lambda=\sum_{j=1}^{s}\lambda_j^k b_j\in\mathcal{D}_{d-1},\ 1\le k\le n. \tag{7.9}$$

Comme $\mathcal{D}_{d-1}$ est stable par dérivation, toutes les dérivées de Λ sont dans $\mathcal{D}_{d-1}$. La dérivation correspond à la multiplication sur les polynômes, donc si $\Lambda(p_i) = 0, 1 \leq i \leq n$, alors $\Lambda(p_i q) = 0$, pour tout $q \in R$, et $\Lambda \in I^\perp$. □
La condition 1 traduit seulement le fait que les *dérivations* $\partial_{\delta_i}, 1 \leq i \leq n$, *commutent ou de manière équivalente que la multiplication dans* $\mathcal{A}$ *est commutative.*

***Exemple* 7.37.** *On considère le point isolé* $0 \in \mathbb{K}^2$ *du système*

$$p_1 = 2\,x_1\,x_2^2 + 5\,x_1^4,\ p_2 = 2\,{x_1}^2\,x_2 + 5\,x_2^4.$$

Pour tout $i, j \in \mathbb{N}$, *on note* $\delta_i^j = \frac{1}{j!}\partial_i^j$. *On vérifie facilement que* $I^\perp$ *contient* $1, \delta_1, \delta_2,\ \delta_1^2, \delta_1\delta_2, \delta_2^2, \delta_1^3,\ \delta_2^3$. *Pour trouver les autres éléments de* $\mathcal{D}$, *on intègre ceux-ci suivant la formule (7.6) en ne gardant que les éléments qui apportent de nouveaux termes*

$$\Lambda = \lambda_1\,\delta_1^4 + \lambda_2\,\delta_1^2\delta_2 + \lambda_3\,\delta_1\delta_2^2 + \lambda_4\,\delta_2^4 + \lambda_5\,\delta_1^3\delta_2 + \lambda_6\,\delta_1\delta_2^3,\ \lambda_i \in \mathbb{K}.$$

Les conditions $\Lambda(p_1) = \Lambda(p_2) = 0$, *entraînent que*

$$\Lambda = \lambda_1(2\,\delta_1^4 - 5\,\delta_1\delta_2^2) + \lambda_2(2\,\delta_2^4 - 5\,\delta_1^2\delta_2)$$

Un nouvel élément de $I^\perp$ *sera (d'après le théorème précédent) de la forme* $\Lambda = \lambda_1\delta_1^5 + \lambda_2(2\,\delta_1^4\delta_2 - 5\,\delta_1\delta_2^3) + \lambda_3(2\,\delta_2^5 - 5\,\delta_1^2\delta_2^2)$ *et ses dérivées doivent être dans l'espace vectoriel engendré par les éléments précédents, ce qui impose que*

$$\Lambda = \lambda\,(5\,\delta_1^2\delta_2^2 - 2\,\delta_1^5 - 2\,\delta_2^5),\ \lambda \in \mathbb{K}.$$

Une nouvelle intégration ne fournit pas d'autre élément dans $\mathcal{D}$ *qui est alors engendré par*

$$1, \delta_1, \delta_2, \delta_1^2, \delta_1\delta_2, \delta_2^2, \delta_1^3, \delta_2^3,$$
$$2\,\delta_1^4 - 5\,\delta_1\delta_2^2, 2\,\delta_2^4 - 5\,\delta_1^2\delta_2, 5\,\delta_1^2\delta_2^2 - 2\,\delta_1^5 - 2\,\delta_2^5.$$

Ceci nous montre que le dual de R/Q_0 *et donc* R/Q_0 *sont de dimension* 11. *Le point* 0 *est donc de multiplicité* 11.

7.2.4. L'algorithme. — Ceci nous conduit naturellement à un algorithme qui construit étape par étape, les générateurs de $\mathcal{D}$. Nous obtiendrons par la même occasion la structure du quotient, c'est-à-dire les matrices de multiplication par les variables x_l ou les matrices de dérivations par $\partial_{\delta_l}, 1 \leq l \leq n$.

***Algorithme* 7.38.** Structure locale d'un point multiple.

Entrée :

$(p_1, \ldots, p_m) \in R^m$ et $\zeta \in \mathbb{K}^n$ tels que $I = (p_1, \ldots, p_m)$ a une composante $\mathfrak{m}_\zeta$-primaire isolée Q_ζ.

▷ $\mathcal{D}_0 := 1$; d := 0 ; s_0 := 1 ; test := vrai ;
Pour k de 1 à n faire $U^k[1]$:= [0] ;
▷ Tant que test faire
1) S := système d'équations 1,2 en λ_j^k ;
2) résoudre le système S ;
3) S'il n'y a pas de nouvelle solution alors test := faux
sinon
soit $(\delta_1, \ldots, \delta_s)$ une base des nouvelles solutions
telle que $\partial_{\delta_k}(\delta_i) = \sum_{j=1}^{s_d} \lambda_{j,s_d+i}\, b_j$;
$s_{d+1} := s_d + s$;
$\mathcal{D}_{d+1} := \mathcal{D}_d, \delta_1, \ldots, \delta_s = b_1, \ldots, b_{s_{d+1}}$;
Pour k de 1 à n faire
Pour i de $s_d + 1$ à s_{d+1} faire
$U^k[i] := [\lambda_{1,i}, \ldots, \lambda_{s_d,i}]$;
$d := d + 1$;
▷ $\mathcal{D}_d$ et U^k pour $1 \le k \le n$;

Sortie :

Une base B de $Q_\zeta^\perp$ dans $\mathbb{K}[\delta_\zeta]$ et les matrices de multiplication par $x_k - \zeta_k$ dans B.

7.2.5. Analyse de la complexité. — Nous détaillons ici l'analyse de complexité de l'algorithme précédent. Une étape importante de cet algorithme est le point (2) que nous allons étudier de plus près. Supposons que nous soiyons au rang d et que nous ayons calculé une base $b_1, \ldots, b_{s_d}$ de $\mathcal{D}_d$. Posons $U_k = (u_{i,j}^k)_{1 \le i,j \le s_d}$ tel que

$$\partial_{\delta_k}(b_j) = \sum_{i=1}^{s_d} u_{i,j}^k\, b_i \quad , \quad 1 \le j \le s_d.$$

Soient $v_l = (\lambda_1^l, \ldots, \lambda_{s_d}^l), 1 \le l \le n$, des vecteurs tels que $V = [v_1, \ldots, v_n]$ soit une solution du système 1, 2 du théorème (7.36). Les équations 1 se réécrivent sous la forme

$$U_k\, v_l - U_l\, v_k = 0,\ 1 \le k < l \le n.$$

Les équations 2 correspondent à

$$[A_1, \ldots, A_n].\, V = 0,$$

où les matrices $A_1, \ldots, A_n$ sont de taille $m \times s_d$ et font intervenir les coefficients des $p_1, \ldots, p_m$. Le système général est donc de la forme

$$\begin{bmatrix}
U_n & & & & -U_1 \\
 & U_n & & & -U_2 \\
 & & \ddots & & \vdots \\
 & & & U_n & -U_{n-1} \\
U_{n-1} & & & -U_1 & \\
 & \ddots & & \vdots & \\
 & & U_{n-1} & -U_{n-2} & \\
\vdots & \vdots & \vdots & & \\
U_2 & -U_1 & & & \\
A_1 & \cdots & \cdots & \cdots & A_n
\end{bmatrix} . V = 0 \ ,$$

où les blancs désignent des 0. C'est un système linéaire de taille $(\frac{1}{2}\, n\, (n-1)\, s_d + m) \times n\, s_d$. Pour résoudre ce système, nous supposons de plus que l'espace vectoriel engendré par les lignes des U_i est inclus dans celui engendré par les lignes de U_n. On peut toujours s'y ramener en prenant pour U_n une combinaison linéaire *générique* des matrices $U_1, \ldots, U_n$ (i.e. on remplace x_n par une combinaison linéaire de $x_1, \ldots, x_n$).

Par élimination de Gauss entre les lignes où intervient U_n et les autres, on remplace les lignes $U_{n-1}\, v_1 - U_1\, v_{n-1} = 0$ par un système de la forme $W_{1,n-1}\, v_n = 0$, où $W_{1,n-1}$ est une matrice de taille $s_d \times s_d$. Le même type de calcul sur les autres $\frac{1}{2}\,(n-1)\,(n-2)+m$ blocs non-nuls permet de transformer le système en un système de taille $(\frac{1}{2}\, n\, (n-1)\, s_d + m) \times s_d$ de la forme $W\, .\, v_n = 0$.

Comme cette matrice est élargie de $s_d - s_{d-1}$ à chaque étape de l'algorithme, on peut supposer que la triangulation des matrices U_n et la réduction ci-dessus sont faites jusqu'au rang s_{d-1}. Le nombre d'étapes nécessaires pour les réductions supplémentaires est donc majoré par $k\, (\frac{1}{2}\, n\, (n-1) + m) \times s_d^2 \times (s_d - s_{d-1})$ (k est une constante). Pour obtenir les nouvelles solutions du système $W\, .\, v_n = 0$, il faut au plus $k'\, (\frac{1}{2}\, n\, (n-1)\, s_d + m) \times s_d\, (s_d - s_{d-1})$ opérations arithmétiques supplémentaires (k' est une constante).

Le nombre total d'opérations pour l'étape 2 est donc majoré par $\mathcal{O}(n^2 \mu^3 + m\, \mu^3)$ où $\mu - 1 = s_\nu - s_0 = (s_1 - s_0) + \cdots + (s_\nu - s_{\nu-1})$.

Voir aussi [**MMM95**] pour une autre approche.

7.3. Interpolation

Les problèmes d'interpolation sont au cœur de beaucoup de méthodes (multiplication rapide de polynômes, approximation par des fonctions polynomiales, splines, ...). Par essence, ce sont des problèmes qui font intervenir la dualité, comme nous allons le détailler dans cette section.

7.3.1. Les polynômes de Lagrange en une variable. — Un problème d'interpolation consiste à reconstruire une fonction à partir de ses valeurs en certains points. Dans le cas classique, étant donnés $d+1$ points *distincts* $t_0, \ldots, t_d \in \mathbb{K}$, et des valeurs $v_0, \ldots, v_d$, on cherche un polynôme p de degré $\leq d$ tel que $p(t_i) = v_i$ ou encore tel que

$$\mathbf{1}_{t_i}(p) = v_i,\ i = 0, \ldots, d.$$

L'unique solution à ce problème est donnée par

$$p = \sum_{i=0}^{d} v_i\, \mathbf{e}_i(t),$$

où

$$\mathbf{e}_i(t) = \prod_{j \neq i} \frac{t - t_j}{t_i - t_j}$$

est le $i^{\text{ème}}$ polynôme de Lagrange. Il vérifie

$$\mathbf{1}_{t_i}(\mathbf{e}_j) = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ sinon} \end{cases}$$

et les familles $(\mathbf{e}_i)_i$ et $(\mathbf{1}_{t_i})_i$ sont donc duales l'une de l'autre. Résoudre ce problème d'interpolation peut aussi s'interpréter comme la résolution du système linéaire suivant :

$$\begin{bmatrix} 1 & t_0 & \ldots & t_0^{d-1} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 1 & t_d & \ldots & t_d^{d-1} \end{bmatrix} \begin{bmatrix} p_0 \\ \vdots \\ \vdots \\ p_{d-1} \end{bmatrix} = \begin{bmatrix} v_0 \\ \vdots \\ \vdots \\ v_{d-1} \end{bmatrix}$$

La matrice ci-dessus $V = (\mathbf{1}_{t_i}(t^j))_{0 \leq i,j \leq d-1}$ est la matrice de Vandermonde des points $t_0, \ldots, t_{d-1}$. C'est aussi la matrice de $\mathbf{1}_{t_0}, \ldots, \mathbf{1}_{t_{d-1}}$ dans la base duale $\mathbf{d}^i$ de la base des monômes. Les coefficients des polynômes de Lagrange dans la base des monômes s'obtiennent à partir des colonnes de l'inverse de cette matrice.

Généralisons cette construction. A la place des évaluations, nous pouvons considérer des formes linéaires quelconques Λ_i, supposées indépendantes. La matrice correspondante est notée $V = (\Lambda_i(t^j))_{0 \leq i,j \leq d-1}$. Si V est inversible, nous pouvons construire la base duale de Λ_i en inversant V : notons $\mathbf{e}_i$ le

polynôme dont les coefficients dans la base monomiale correspondent à la i^{ème} colonne de V^{-1}. On a alors

$$\Lambda_j(\mathbf{e}_i) = \delta_{i,j}$$

et $(\mathbf{e}_i)_{0\le i\le d-1}$ est donc la base duale de $(\Lambda_i)_{0\le i\le d-1}$. Une solution du problème d'interpolation

$$\Lambda_i(p) = v_i, i = 0, \dots, d-1 \tag{7.10}$$

est alors

$$p(t) = \sum_{i=0}^{d} v_i\, \mathbf{e}_i(t).$$

Supposons ici que $t\cdot\Lambda_i \in \langle\Lambda_j\rangle_{j=0,\dots,d-1}$. Nous pouvons alors caractériser toutes les solutions du problème (7.10). En effet, de l'hypothèse précédente, nous déduisons (voir lemme 7.14) que $\mathcal{D}^\perp = \{p \in \mathbb{K}[t];\ \Lambda_i(p) = 0,\ i = 0, \dots, d-1\}$ est un idéal de $\mathbb{K}[t]$, donc principal. Pour calculer son générateur g, nous procédons de la façon suivante :

Remarquons d'abord que g est de degré d car $\mathbb{K}[t]/\mathcal{D}^\perp = \mathbb{K}[t]/(g)$ est une algèbre quotient dont le dual $\langle\Lambda_j\rangle_{j=0,\dots,d-1}$ est de dimension d.

Par ailleurs, le vecteur $[g_0, \dots, g_{d-1}, 1]$ des coefficients de $g = g_0 + \cdots + g_{d-1}\, t^{d-1} + t^d$ est dans le noyau de

$$\tilde{V} = \begin{bmatrix} \Lambda_0(1) & \cdots & \Lambda_0(t^d) \\ \vdots & & \vdots \\ \Lambda_{d-1}(1) & \cdots & \Lambda_{d-1}(t^d) \end{bmatrix}.$$

En multipliant à gauche cette matrice par $V^{-\mathtt{t}(1)}$, nous ne changeons pas le noyau et nous obtenons donc

$$V^{-\mathtt{t}}\,\tilde{V} = \begin{bmatrix} 1 & & 0 & -g_0 \\ & \ddots & & \vdots \\ 0 & & 1 & -g_{d-1} \end{bmatrix}.$$

Ce qui nous donne les formules :

$$[g_i]_{0\le i\le d-1} = -V^{-\mathtt{t}}\,[\Lambda_i(t^n)]_{0\le i\le d-1}$$

***Exemple* 7.39.** *Un exemple d'un tel problème est* le problème d'interpolation d'Hermite *:*

$$p^{(l)}(t_i) = v_{i,l},\ l = 0, \dots, k_i, i = 0, \dots, e.$$

Les formes linéaires Λ_l *sont les*

$$\mathbf{d}^l_{t_i},\ l = 0, \dots, k_i, i = 0, \dots, e.$$

(1) Pour toute matrice M inversible, $M^{-\mathtt{t}}$ est la transposée de l'inverse de M

Remarquons que

$$t \cdot \mathbf{d}_{t_i}^l = t_i\, \mathbf{d}_{t_i}^l + \mathbf{d}_{t_i}^{l-1},$$

ce qui nous montre que cet espace de formes linéaires est stable par dérivation et que son orthogonal $I(\Lambda)$ est un idéal engendré par le polynôme $g = g_0 + \cdots + g_{d-1}\, x^{d-1} + x^d$ tel que $[g_i]_{0\le i\le d-1}$ vaut

$$- \left[\begin{array}{cccc} 1 & t_0 & \cdots & t_0^{d-1} \\ 0 & 1 & \cdots & (d-1)\, t_0^{d-2} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & (d-1)\cdots(d-k_0) t_0^{d-k_0-1} \\ \hline \vdots & \vdots & \vdots & \vdots \\ \hline 1 & t_{d-1} & \cdots & t_{d-1}^{d-1} \\ 0 & 1 & \cdots & (d-1)\, t_{d-1}^{d-2} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & (d-1)\cdots(d-k_{d-1}) t_{d-1}^{d-k_{d-1}-1} \end{array}\right]^{-\mathtt{t}} \left[\begin{array}{c} t_0^d \\ d\, t_0^{d-1} \\ \vdots \\ \frac{d!}{(d-k_0)!} t_0^{d-k_0} \\ \vdots \\ t_{d-1} \\ d\, t_{d-1}^{d-1} \\ \vdots \\ \frac{d!}{(d-k_{d-1})!} t_{d-1}^{d-k_{d-1}} \end{array}\right]$$

7.3.2. Le cas de plusieurs variables. — Nous pouvons généraliser cette approche au cas de plusieurs variables. Considérons D formes linéaires $\Lambda_1, \ldots, \Lambda_D$ indépendantes de $\widehat{\mathbb{K}[\mathbf{x}]}$. Le problème d'interpolation consiste, étant données D valeurs $v_i, i = 1, \ldots, D$ à calculer les polynômes $p \in \mathbb{K}[\mathbf{x}]$ tels que

$$\Lambda_i(p) = v_i,\ i = 1, \ldots, D. \tag{7.11}$$

Le cas classique correspondant au cas d'évaluations $\Lambda_i = \mathbf{1}_{\zeta_i}$ en des points $\zeta_i \in \mathbb{K}^n$ $(i = 1, \ldots, D)$ sera détaillé dans les sections suivantes. Le cas général correspond à des conditions tangentielles (sur les dérivées) en des points $\zeta_i, i = 1, \ldots, d$, les Λ_j étant des fonctions de dérivations en ζ_i. Ce problème est également appelé problème *d'interpolation d'Hermite.*

***Exemple* 7.40.** *Un tel problème est défini sur $\mathbb{K}[x_1, x_2]$, par exemple, par*

$$\begin{array}{l} \langle 1, p\rangle_{(0,0)} = v_1,\ \langle \mathbf{d}_1, p\rangle_{(0,0)} = v_2,\ \langle \mathbf{d}_2, p\rangle_{(0,0)} = v_3, \\ \langle 1, p\rangle_{(1,1)} = v_4,\ \langle \mathbf{d}_1, p\rangle_{(1,1)} = v_5,\ \langle \mathbf{d}_1^2, p\rangle_{(1,1)} = v_6, \end{array}$$

$v_i \in \mathbb{K}$, $p \in \mathbb{K}[x_1, x_2]$.

Pour $\Lambda = \{\Lambda_1, \ldots, \Lambda_D\}$, nous noterons aussi

$$I(\Lambda) = \{p \in \mathbb{K}[\mathbf{x}];\ \text{tel que } \lambda(p) = 0,\ \forall \lambda \in \Lambda\}$$

si Λ est stable. Nous allons décrire la structure du quotient $\mathbb{K}[\mathbf{x}]/I(\Lambda)$.

Pour tout ensemble de monômes $\mathbf{x}^E = \{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D}\}$, notons

$$\Lambda(\mathbf{x}^E) = [\Lambda_i(\mathbf{x}^{\alpha_j})]_{1\le i,j\le D}.$$

Ces matrices généralisent les matrices de Vandermonde aux cas de plusieurs variables [**MP00**].

***Proposition* 7.41.** *Supposons que les formes linéaires $\Lambda_i, i = 1, \ldots, D$, sont indépendantes et notons $\Lambda = \{\Lambda_1, \ldots, \Lambda_D\}$. Alors, $\mathbf{x}^E$ est une base de $R/I(\Lambda)$ si et seulement si $V = \Lambda(\mathbf{x}^E) = [\Lambda_i(\mathbf{x}^\alpha)]_{i=1,\ldots,D,\ \alpha\in E}$ est inversible.*

Démonstration. Comme $I(\Lambda)^\perp = \langle\Lambda\rangle$ est un espace vectoriel de dimension D (les formes linéaires Λ_i étant supposées indépendantes), $R/I(\Lambda)$ est un espace vectoriel de dimension D. L'ensemble de monômes $\mathbf{x}^E$ est une base de $R/I(\Lambda)$ si et seulement si les vecteurs des valeurs des formes linéaires Λ_j sur ces monômes sont indépendants, c'est-à-dire ssi la matrice $\Lambda(\mathbf{x}^E)$ est inversible. □

Supposons connu un tel ensemble $\mathbf{x}^E$ tel que $\Lambda(\mathbf{x}^E)$ soit inversible. Construisons alors $(\mathbf{e}_j(\mathbf{x})) \in \mathbb{K}[\mathbf{x}], j = 1, \ldots, D$ tels que

$$\Lambda_i(\mathbf{e}_j) = \delta_{i,j}.$$

Le vecteur des coefficients de $\mathbf{e}_i$ dans la base des monômes $(\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D})$ est donné par la $i^{\text{ème}}$ colonne de $V^{-1} = \Lambda(\mathbf{x}^E)^{-1}$.

***Proposition* 7.42.** *L'unique solution à support dans $\langle\mathbf{x}^E\rangle$ du problème d'interpolation (7.11) est*

$$p = \sum_{i=0}^{D} v_i\, \mathbf{e}_i(\mathbf{x}).$$

Démonstration. Le polynôme $p = \sum_{i=0}^{D} v_i\, \mathbf{e}_i(\mathbf{x})$ vérifie $\Lambda_j(p) = v_j$. Comme $\mathbf{x}^E$ est une base de $\mathbb{K}[\mathbf{x}]/I(\Lambda)$, c'est l'unique polynôme à support dans $\langle\mathbf{x}^E\rangle$ vérifiant ces contraintes. □

Les autres solutions du problème (7.11) sont de la forme $p + I(\Lambda)$. Remarquons également que nous avons

$$I(\Lambda) = \langle \mathbf{x}^\beta - \sum_{i=0}^{D} \Lambda_i(\mathbf{x}^\beta)\, \mathbf{e}_i(\mathbf{x}), \beta \in \mathbb{N}^n \rangle.$$

7.3.3. Une base d'interpolation. — Nous considérons toujours ici le cas général d'un ensemble de D formes linéaires indépendantes $\Lambda_1, \ldots, \Lambda_D$, formant un sous-espace stable. Pour résoudre les problèmes d'interpolation, nous avons besoin de connaître un ensemble $\mathbf{x}^E = \{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D}\}$ formant une base de $I(\Lambda)$. Nous allons voir ici comment le construire algorithmiquement. L'idée simple à la base de cet algorithme est de construire, de manière incrémentale, cette base en partant du monôme 1, en multipliant par les variables $x_1, \ldots, x_n$ et en testant l'indépendance dans $\mathbb{K}[\mathbf{x}]/I(\Lambda)$ des nouveaux monômes, que l'on rajoute, en leur appliquant les formes linéaires Λ.

Pour tout polynôme $p \in \mathbb{K}[\mathbf{x}]$, notons $\Lambda(p) = [\Lambda_1(p), \ldots, \Lambda_D(p)]$ et pour tout ensemble de polynômes $\mathcal{M}$, notons $\mathcal{M}^+ = \mathcal{M} \cup x_1\mathcal{M} \cup \cdots \cup x_n\mathcal{M}$.

***Algorithme* 7.43.** Base d'interpolation et relations.

Entrée : Le système inverse Λ, $\mathcal{M} := \{1\}$, $L := \{\Lambda(1)\}$, $B := \{1\}$, $G := \{\}$.

1. Calculer $\mathcal{M} := \mathcal{M}^+ \backslash \mathcal{M}$.
2. Tant que $\mathcal{M} \neq \emptyset$, pour tout monôme $t \in \mathcal{M}$,
   (a) calculer $\Lambda(m)$,
   (b) Si $\Lambda(t) \in \langle L \rangle = \langle \Lambda(m_1), \ldots, \Lambda(m_k) \rangle$, c'est-à-dire s'il existe $a_i \in \mathbb{K}$ tels que
   $$\Lambda(t) = \sum_i a_i \, \Lambda(m_i),$$
   rajouter $r = t - \sum_{j=1}^{k} a_j \, m_j$ à G et enlever t de $\mathcal{M}$.
   (c) Sinon rajouter $\Lambda(t)$ à L et t à B.
   (d) Calculer $\mathcal{M} := \mathcal{M}^+ \backslash \mathcal{M}$.

Sortie : L'ensemble B est une base de $\mathbb{K}[\mathbf{x}]/I(\Lambda)$ et G l'ensemble des relations permettant de réécrire tout polynôme de B^+ dans $\langle B \rangle$.

Cet algorithme s'arrête nécessairement car l'ensemble des monômes B est tel que $\Lambda(B)$ est de rang $|B| \leq D$. Il ne peut donc croître indéfiniment. Par construction, l'ensemble B est connexe à 1 (tout monôme de m est connecté à 1 par un chemin de multiplication par les variables restant dans B). Si B est de taille $D' < D$, tout monôme de B^+ se réécrivant dans B modulo $G \subset I(\Lambda)$, nous obtenons une partie génératrice B de $\mathbb{K}[\mathbf{x}]/I(\Lambda)$ de taille $D' < D = \dim_{\mathbb{K}}(\mathbb{K}[\mathbf{x}]/I(\Lambda))$, ce qui est contradictoire. Quand l'algorithme s'arrête, B est donc un ensemble de D monômes indépendants de $\mathbb{K}[\mathbf{x}]/I(\Lambda)$, c'est-à-dire une base. De plus, les relations G permettent de réécrire tout monôme de B^+ dans $\langle B \rangle$.

***Exemple* 7.44.** *Soient* $\zeta_1 = (0,0), \zeta_2 = (1,0) \in \mathbb{K}^2$, $\Lambda = \{\mathbf{1}_{\zeta_1}, \mathbf{1}_{\zeta_2}, \mathbf{d}_{\zeta_2}^{(1,0)}\}$. *A la première étape, nous calculons*

$$\Lambda(1) = [1, 1, 0].$$

A la deuxième étape, $\mathcal{M} := \{x_1, x_2\}$

$$\Lambda(x_1) = [0, 1, 1], \Lambda(x_2) = [0, 0, 0],$$

et $G := \{x_2\}$, $B := \{1, x_1\}$, $\mathcal{M} := \{x_1\}$. *A l'étape suivante,*

$$\Lambda(x_1^1) = [0, 1, 0], \Lambda(x_1 \, x_2) = [0, 0, 0],$$

et $G := \{x_2, x_1\, x_2\}$, $B := \{1, x_1, x_1^2\}$, $\mathcal{M} := \{x_1^2\}$. *Enfin la dernière étape donne*

$$\Lambda(x_1^3) = [0,1,0], \Lambda(x_1^2\, x_2) = [0,0,0],$$

et $G := \{x_2, x_1x_2, x_1^3 - x_1^2\}$, $B := \{1, x_1, x_1^2\}$ *et* $\mathcal{M} := \{\}$.

Nous obtenons ainsi la base d'interpolation $B = \{1, x_1, x_1^2\}$ *et l'idéal* $(x_2, x_1^3 - x_1^2)$ *associé aux points* $(0,0)$ *et* $(0,1)$ *de multiplicité* 2.

Cet algorithme peut être optimisé de plusieurs façons. Si nous voulons calculer une base de Gröbner pour un ordre donné, nous trions également les monômes de $\mathcal{M}$ suivant cet ordre et nous ne considérons dans $\mathcal{M}^+$ que les monômes en dehors de l'initial de G. Les relations de G ainsi construites formeront alors une base de Gröbner réduite.

Dans le test d'appartenance à $\langle L\rangle$ et le calcul des a_i (étape 2.b), l'utilisation de la triangularisation partielle de L permet de répondre de manière rapide (en $\mathcal{O}(|L|^2)$) à ce problème. Ce qui conduit à une complexité globale en $\mathcal{O}(D^3)$ opérations arithmétiques.

Remarquons aussi que le calcul de $\Lambda(x_i\, m)$ peut se faire facilement dans certains cas (par exemple, pour des évaluations) à partir de $\Lambda(m)$.

Nous allons maintenant détailler ces constructions dans le cas d'un problème d'interpolation en des points simples.

7.3.4. L'interpolation en des points simples. — Nous considérons ici les D formes linéaires d'évaluation $\Lambda_i = \mathbf{1}_{\zeta_i}$ en les points $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_D\} \subset \mathbb{K}^n$. Nous cherchons à répondre au problème d'interpolation (7.11).

Pour cela, nous supposons connu un ensemble $\mathbf{x}^E = \{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D}\}$ tel que $\Lambda(\mathbf{x}^E)$ soit inversible et nous construisons les D polynômes $\mathbf{e}_1(\mathbf{x}), \ldots, \mathbf{e}_D(\mathbf{x}) \in \mathbb{K}[\mathbf{x}]$ tels que

$$\Lambda_i(\mathbf{e}_j) = \delta_{i,j},$$

en inversant la matrice $V = \Lambda(\mathbf{x}^E)$.

***Définition* 7.45.** *Pour tout ensemble* $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_D\} \subset \mathbb{K}^n$, *nous notons* $\mathcal{I}(\mathcal{Z})$ *l'idéal des polynômes s'annulant en ces points.*

***Proposition* 7.46.** *Les* $(\mathbf{e}_i)_{i=1,\ldots,D}$ *forment un système d'idempotents orthogonaux de* $\mathbb{K}[\mathbf{x}]/\mathcal{I}(\mathcal{Z})$.

Démonstration. Comme $\mathbf{1}_{\zeta_i}(\mathbf{e}_j) = \delta_{i,j}$, on a pour tout $i, j, k \in \{1, \ldots, D\}$,

- $\mathbf{1}_{\zeta_i}(\mathbf{e}_j^2 - \mathbf{e}_j) = 0$,
- $\mathbf{1}_{\zeta_i}(\mathbf{e}_j\, \mathbf{e}_k) = 0$, $j \neq k$,
- $\mathbf{1}_{\zeta_i}(\sum_{j=1}^D \mathbf{e}_j - 1) = 0$.

On en déduit les égalités suivantes dans $\mathcal{A}_\mathcal{Z} = \mathbb{K}[\mathbf{x}]/\mathcal{I}(\mathcal{Z})$:

- $\mathbf{e}_j^2 - \mathbf{e}_j \equiv 0$,
- $\mathbf{e}_j\, \mathbf{e}_k \equiv 0$, $j \neq k$,

– $\sum_{j=1}^{D} \mathbf{e}_j \equiv 1$,
et $(\mathbf{e}_i)_{i=1,\ldots,D}$ est bien un système d'idempotents orthogonaux de $\mathbb{K}[\mathbf{x}]/\mathcal{I}(\mathcal{Z})$.
□

***Proposition* 7.47.** *L'idéal $\mathcal{I}(\mathcal{Z})$ est radical.*

Démonstration. En effet,

$$\begin{aligned}\mathcal{I}(\mathcal{Z}) &= \{p \in \mathbb{K}[\mathbf{x}]; p(\zeta_i) = 0,\ i = 1, \ldots, D\} \\ &= \mathcal{I}(\{\zeta_1, \ldots, \zeta_D\}) = \mathcal{I}(\mathcal{V}(\mathcal{I}(\{\zeta_1, \ldots, \zeta_D\}))) \\ &= \sqrt{\mathcal{I}(\{\zeta_1, \ldots, \zeta_D\})} = \sqrt{\mathcal{I}(\mathcal{Z})},\end{aligned}$$

d'après le théorème des Zéros de Hilbert. □

***Proposition* 7.48.** *Soient U et $V \subset U$ deux sous-ensembles de $\mathbb{K}^n$.*

$$\mathcal{I}(U - V) = \mathcal{I}(U) + (\sum_{b \in V} \mathbf{e}_b(\mathbf{x})) = \mathcal{I}(U) + \sum_{b \in V} (\mathbf{e}_b(\mathbf{x})).$$

Démonstration. Comme $\mathbf{e}_a \mathbf{e}_{a'} \equiv 0$ si $a \neq a'$ et $\mathbf{e}_a^2 \equiv \mathbf{e}_a$ modulo $\mathcal{I}(U)$, on a bien

$$\mathbb{K}[\mathbf{x}]/(\mathcal{I}(U) + (\sum_{b \in V} \mathbf{e}_b(\mathbf{x}))) = \mathbb{K}[\mathbf{x}]/(\mathcal{I}(U) + \sum_{b \in V} (\mathbf{e}_b(\mathbf{x}))).$$

Par ailleurs, remarquons que pour tout U, $\mathbb{K}[\mathbf{x}]/\mathcal{I}(U) = \oplus_{a \in U} \langle \mathbf{e}_a \rangle$ et donc que

$$\mathbb{K}[\mathbf{x}]/(\mathcal{I}(U) + \sum_{b \in V} (\mathbf{e}_b(\mathbf{x}))) = \oplus_{a \in U - V} \langle \mathbf{e}_a \rangle = \mathbb{K}[\mathbf{x}]/\mathcal{I}(U - V),$$

d'où l'égalité entre les idéaux. □

***Proposition* 7.49.** *L'idéal $\mathcal{I}(U)$ est engendré par au plus $n + 1$ polynômes.*

Démonstration. Pour $i = 1, \ldots, n$, notons $p_i(x_i)$ le polynôme de l'idéal $\mathcal{I}(U)$, de degré minimal et qui s'annule sur toutes les $i^{\text{ème}}$ coordonnées des points de U. Les points de $W = \mathcal{Z}(p_1, \ldots, p_n)$ sont sur une grille contenant l'ensemble U. Notons $V = W - U$. D'après ci-dessus, on a donc

$$\mathcal{I}(U) = \mathcal{I}(W - V) = \mathcal{I}(W) + (\sum_{b \in V} \mathbf{e}_b(\mathbf{x})) = (p_1(x_1), \ldots, p_n(x_n), \sum_{b \in V} \mathbf{e}_b(\mathbf{x}))$$

qui est bien engendré par au plus $n + 1$ polynômes. □
Cette proposition nous dit que tout ensemble de points dans un espace de dimension n peut être défini par $n + 1$ équations.

Pour plus de détails sur ces idéaux de points, voir aussi [**Rob00**], [**Las01**].

7.3.5. Relations entre coefficients et racines. — Nous considérons ici encore D points distincts $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_D\}$ de $\mathbb{K}^n$. Notons $\mathcal{A}_\mathcal{Z} = R/\mathcal{I}(\mathcal{Z})$ l'anneau quotient de $\mathbb{K}[\mathbf{x}]$ par $\mathcal{I}(\mathcal{Z})$ (l'idéal des polynômes s'annulant en $\mathcal{Z}$). C'est donc un espace vectoriel de dimension D dont une base du dual est la base des évaluations $(\mathbf{1}_{\zeta_i})_{i=1,\ldots,D}$ en les points ζ_i.

Notons $(\mathbf{x}^{\alpha_i})_{i=1,\ldots,D}$ une base du quotient $\mathcal{A}_\mathcal{Z}$. Nous savons alors (proposition 7.41) que le déterminant

$$V_E(\mathcal{Z}) = \begin{vmatrix} \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_D} \\ \vdots & \vdots & \vdots \\ \zeta_D^{\alpha_1} & \cdots & \zeta_D^{\alpha_D} \end{vmatrix}$$

n'est pas nul. Ce déterminant généralise le déterminant de Vandermonde en une variable [**MP00**]. Nous allons nous en servir pour décrire les idempotents de $\mathcal{A}_\mathcal{Z}$. Pour cela notons

$$V_{i,E}(\mathcal{Z}, \mathbf{x}) = \begin{vmatrix} \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_D} \\ \vdots & \vdots & \vdots \\ \zeta_{i-1}^{\alpha_1} & \cdots & \zeta_{i-1}^{\alpha_D} \\ \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ \zeta_{i+1}^{\alpha_1} & \cdots & \zeta_{i+1}^{\alpha_D} \\ \vdots & \vdots & \vdots \\ \zeta_D^{\alpha_1} & \cdots & \zeta_D^{\alpha_D} \end{vmatrix}.$$

***Proposition* 7.50.** *L'idempotent de $\mathcal{A}_\mathcal{Z}$ associé à la racine ζ_i est*

$$\mathbf{e}_i(\mathcal{Z}, \mathbf{x}) = \frac{V_{i,E}(\mathcal{Z}, \mathbf{x})}{V_E(\mathcal{Z})}.$$

Démonstration. Nous vérifions que $\mathbf{e}_i(\mathcal{Z}\, x)$ est une combinaison linéaire des monômes $(\mathbf{x}^{\alpha_i})_{i=1,\ldots,D}$ formant une base de $\mathcal{A}_\mathcal{Z}$ telle que

- $\mathbf{e}_i(\mathcal{Z}, \mathbf{x})(\zeta_j) = 0$ si $i \neq j$, et
- $\mathbf{e}_i(\mathcal{Z}, \mathbf{x})(\zeta_i) = 1$.

Ceci caractérise le polynôme de l'espace vectoriel $\langle \mathbf{x}^{\alpha_i} \rangle_{i=1,\ldots,D}$ définissant l'idempotent de $\mathcal{A}_\mathcal{Z}$ associé à ζ_i. □

Ces matrices de Vandermonde généralisées vont nous permettre également de calculer explicitement la forme normale d'un polynôme. Notons

$$R_Q(\mathcal{Z}, \mathbf{x}) = \begin{vmatrix} Q(\mathbf{x}) & \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ Q(\zeta_1) & \zeta_1^{\alpha_1} & \cdots & \zeta_1^{\alpha_D} \\ \vdots & \vdots & \vdots & \vdots \\ Q(\zeta_D) & \zeta_D^{\alpha_1} & \cdots & \zeta_D^{\alpha_D} \end{vmatrix}.$$

***Proposition* 7.51.** *La forme normale de Q dans la base $\langle \mathbf{x}^E \rangle$ de $\mathcal{A}_\mathcal{Z}$ est*

$$N_Q(\mathbf{x}) = Q - \frac{1}{V_E(\mathcal{Z})} R_Q(\mathcal{Z}, \mathbf{x}). \tag{7.12}$$

Démonstration. Remarquons que $R_Q(\mathcal{Z}, \zeta_i) = 0$ pour $i = 1, \ldots, D$ et donc que $R_Q(\mathcal{Z}, \zeta_i) \equiv 0$ dans $\mathcal{A}_\mathcal{Z}$. De plus, en développant le déterminant suivant la première colonne, $\frac{1}{V_E(\mathcal{Z})} R_Q(\mathcal{Z}, \mathbf{x}) = Q(\mathbf{x}) - N_Q(\mathbf{x})$ où $N_Q(\mathbf{x}) \in \langle \mathbf{x}^{\alpha_i} \rangle_{i=1,\ldots,D}$. Nous en déduisons donc que $Q(\mathbf{x}) \equiv N_Q(\mathbf{x})$, c'est-à-dire que $N_Q(\mathbf{x})$ est la forme normale de Q dans la base $\langle \mathbf{x}^E \rangle$ de $\mathcal{A}_\mathcal{Z}$. □

La formule (7.12) est, en un certain sens, une généralisation en plusieurs variables des relations entre les coefficients et racines. En effet, appliquons-la pour une variable, d points de $\mathbb{K}$, $\mathcal{Z} = \{z_1, \ldots, z_d\} \in \mathbb{K}$, et $Q = x^d$. Nous obtenons

$$\frac{1}{V_E(\mathcal{Z})} R_Q(\mathcal{Z}, \mathbf{x}) = \prod_i (x - z_i) = x^d + \sum_{i=1}^{d} (-1)^i S_i(\mathcal{Z}) x^i$$

où

$$S_i(z_1, \ldots, z_d) = \frac{\begin{vmatrix} 1 & z_1 \cdots z_1^{i-1} & z_1^{i+1} \cdots z_1^{d-1} & z_1^d \\ \vdots & \vdots & \vdots & \vdots \\ 1 & z_d \cdots z_d^{i-1} & z_d^{i+1} \cdots z_d^{d-1} & z_d^d \end{vmatrix}}{\begin{vmatrix} 1 & z_1 & \cdots & z_1^{d-1} \\ \vdots & \vdots & \vdots & \\ 1 & z_d & \cdots & z_d^{d-1} \end{vmatrix}}$$

est la $i^{\text{ème}}$ fonction symétrique des racines. En effet, c'est une fonction symétrique en $z_1, \ldots, z_d$, de degré 1 en chaque z_i et de degré total $d - i$. C'est donc $\sigma_i(z_1, \ldots, z_d) = \sum_{j_1 < \cdots < j_{d-i}} z_{j_1} \cdots z_{j_{d-i}}$.

7.3.6. La méthode de Weierstrass. — Nous venons de voir comment, étant donnés D points $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_D\}$, calculer la forme normale d'un polynôme et les idempotents associés à ces racines. Cependant en pratique, c'est généralement le problème **inverse** qui nous intéresse, à savoir, déterminer les racines à partir de la forme normale d'un certain nombre de polynômes. Nous cherchons donc D points $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_D\} \subset \overline{\mathbb{K}}^n$ tels que pour tout Q,

$$Q(\mathbf{x}) - \frac{1}{V_E(\mathcal{Z})} R_Q(\mathcal{Z}, \mathbf{x}) = N_Q(\mathbf{x}). \tag{7.13}$$

Supposons que nous cherchons à calculer les points distincts et simples $\mathcal{Z} = \{\zeta_1, \ldots, \zeta_D\}$ définis par les n équations $f_1(\mathbf{x}) = 0, \ldots, f_n(\mathbf{x}) = 0$. Supposons

également connue une base $\mathbf{x}^E = \{\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_D}\}$ de $\mathcal{A} = \mathbb{K}[\mathbf{x}]/(f_1, \ldots, f_n) = \mathcal{A}_{\mathcal{Z}}$. Pour chaque $i = 1, \ldots, n$, nous avons $N_{f_i}(\mathbf{x}) = 0$ et chaque relation

$$f_i(\mathbf{x}) - \frac{1}{V_E(\mathbf{u})} R_{f_i}(\mathbf{u}, \mathbf{x}) = 0$$

impose D relations en $\mathbf{u}$, vérifiées pour $\mathbf{u} = \zeta$. Comme $\mathbf{u}$ dépend de $n \times D$ coordonnées, nous obtenons donc un système $F_{\mathbf{f}}(\mathbf{u}) = 0$ (avec $\mathbf{f} = (f_1, \ldots, f_n)$) à $n \times D$ contraintes en les $n \times D$ inconnues $\mathbf{u}$. Nous allons, dans un premier temps, lui appliquer la méthode de Newton pour calculer localement les racines à partir d'une approximation. Le nouveau point après une itération de la méthode de Newton en $\mathbf{u}$ est donc :

$$\mathbf{u}' := \mathbf{u} - J_{F_{\mathbf{f}}}(\mathbf{u})^{-1} F_{\mathbf{f}}(\mathbf{u}),$$

sous réserve que la matrice jacobienne $J_{F_{\mathbf{f}}}$ de $F_{\mathbf{f}}$ par rapport à $\mathbf{u}$ soit inversible. Dans le cas d'une variable ($\mathbf{u} = \{u_1, \ldots, u_d\}$ avec $u_i \in \overline{\mathbb{K}}$), ceci nous conduit à la méthode de Weierstrass [**Wei03**] (énoncée sous la forme qui suit par Durand-Kerner [**Ker66, Dur68**]). L'inverse du Jacobien peut être calculé explicitement et l'itération s'écrit, composante par composante,

$$u_i' := u_i - \frac{f(u_i)}{\prod_{j \neq i}(u_i - u_j)}, \ i = 1, \ldots, D. \tag{7.14}$$

Cette méthode et ses généralisations (Aberth [**Abe73**]) sont à la base d'une méthode de résolution de polynômes en une variable très performante [**Bin96**]. Nous allons voir comment généraliser cette méthode en plusieurs variables.

Notons $F_Q(\mathbf{u}, \mathbf{x}) = Q(\mathbf{x}) - \frac{1}{V_E(\mathbf{u})} R_Q(\mathbf{u}, \mathbf{x})$. Nous cherchons donc à vérifier l'ensemble des $n \times D$ contraintes en $\mathbf{u}$, induites par les polynômes R_{f_i}, $i = 1, \ldots, n$.

***Proposition* 7.52.** *Pour $k = 1, \ldots, n$,*

$$\partial_{u_{i,j}}(F_{f_k})(\mathbf{u}, \mathbf{x}) = \frac{1}{V_E(\mathbf{u})} \partial_{x_i}(R_{f_k})(\mathbf{u}, \mathbf{u}_j) \mathbf{e}_{\mathbf{u}_j}(\mathbf{u}, \mathbf{x}).$$

Démonstration. Pour tout polynôme $Q \in \mathbb{K}[\mathbf{x}]$, nous avons

$$\partial_{u_{i,j}}(F_Q)(\mathbf{u}, \mathbf{x}) = -\frac{1}{V_E(\mathbf{u})} \partial_{u_{i,j}}(R_Q)(\mathbf{u}, \mathbf{x}) + \frac{\partial_{u_{i,j}}(R_Q)(\mathbf{u}, \mathbf{x})}{V_E(\mathbf{u})^2} R_Q(\mathbf{u}, \mathbf{x}). \tag{7.15}$$

Considérons en particulier

$$\partial_{u_{i,j}}(R_Q)(\mathbf{u},\mathbf{x}) = \begin{vmatrix} Q(\mathbf{x}) & \mathbf{x}^{\alpha_1} & \cdots & \mathbf{x}^{\alpha_D} \\ Q(\mathbf{u}_1) & \mathbf{u}_1^{\alpha_1} & \cdots & \mathbf{u}_1^{\alpha_D} \\ \vdots & \vdots & \vdots & \vdots \\ Q(\mathbf{u}_{i-1}) & \mathbf{u}_{i-1}^{\alpha_1} & \cdots & \mathbf{u}_{i-1}^{\alpha_D} \\ \partial_{u_{i,j}}(Q)(\mathbf{u}_i) & \alpha_{1,j}\,\mathbf{u}_i^{\alpha_1-\eta_j} & \cdots & \alpha_{D,j}\,\mathbf{u}_i^{\alpha_D-\eta_j} \\ Q(\mathbf{u}_{i+1}) & \mathbf{u}_{i+1}^{\alpha_1} & \cdots & \mathbf{u}_{i+1}^{\alpha_D} \\ \vdots & \vdots & \vdots & \vdots \\ Q(\mathbf{u}_D) & \mathbf{u}_D^{\alpha_1} & \cdots & \mathbf{u}_D^{\alpha_D} \end{vmatrix}.$$

Nous avons alors $\partial_{u_{i,j}}(R_Q)(\mathbf{u},\mathbf{u}_k) = 0$ pour tout $k \neq i$. D'après la formule (7.15), nous avons de même $\partial_{u_{i,j}}(F_Q)(\mathbf{u},\mathbf{u}_k) = 0$ pour tout $k \neq i$. De plus

$$\begin{aligned} \partial_{u_{i,j}}(R_Q)(\mathbf{u},\mathbf{u}_i) &= -\begin{vmatrix} \partial_{x_j}(Q)(\mathbf{u}_i) & \alpha_{1,j}\,\mathbf{u}_i^{\alpha_1-\eta_j} & \cdots & \alpha_{D,j}\,\mathbf{u}_i^{\alpha_D-\eta_j} \\ Q(\mathbf{u}_1) & \mathbf{u}_1^{\alpha_1} & \cdots & \mathbf{u}_1^{\alpha_D} \\ \vdots & \vdots & \vdots & \vdots \\ Q(\mathbf{u}_{i-1}) & \mathbf{u}_{i-1}^{\alpha_1} & \cdots & \mathbf{u}_{i-1}^{\alpha_D} \\ Q(\mathbf{u}_i) & \mathbf{u}_i^{\alpha_1} & \cdots & \mathbf{u}_i^{\alpha_D} \\ Q(\mathbf{u}_{i+1}) & \mathbf{u}_{i+1}^{\alpha_1} & \cdots & \mathbf{u}_{i+1}^{\alpha_D} \\ \vdots & \vdots & \vdots & \vdots \\ Q(\mathbf{u}_D) & \mathbf{u}_D^{\alpha_1} & \cdots & \mathbf{u}_D^{\alpha_D} \end{vmatrix} \\ &= -\partial_{x_j}(R_Q)(\mathbf{u},\mathbf{u}_i), \end{aligned}$$

où η_j est le j$^{\text{ème}}$ vecteur de la base canonique de $\mathbb{K}^n$. D'après (7.15), nous avons aussi

$$\partial_{u_{i,j}}(F_Q)(\mathbf{u},\mathbf{u}_i) = \frac{\partial_{x_j}(R_Q)(\mathbf{u},\mathbf{u}_i)}{V_E(\mathbf{u})}.$$

Remarquons de plus que

$$\begin{aligned} \partial_{u_{i,j}}F_Q)(\mathbf{u},\mathbf{x}) &= \partial_{u_{i,j}}(Q(\mathbf{x}) - N_Q(\mathbf{u},\mathbf{x})) \\ &= -\partial_{u_{i,j}}(N_Q)(\mathbf{u},\mathbf{x}) \end{aligned}$$

et que $\partial_{u_{i,j}}(F_Q)(\mathbf{u},\mathbf{x})$ est une combinaison linéaire des monômes $\mathbf{x}^{\alpha_1},\ldots,\mathbf{x}^{\alpha_D}$. Le polynôme $\partial_{u_{i,j}}(F_Q)(\mathbf{u},\mathbf{x})$ s'annule en tous les points $\mathbf{u}_k$, $k \neq i$, vaut $-\frac{\partial_{x_j}(R_Q)(\mathbf{u},\mathbf{u}_i)}{V_E(\mathbf{u})}$ en $\mathbf{u}_i$ et a le même support que $\mathbf{e}_i(\mathbf{u},x)$. On en déduit donc que

$$\partial_{u_{i,j}}(F_Q)(\mathbf{u},\mathbf{x}) = \frac{\partial_{x_j}(R_Q)(\mathbf{u},\mathbf{u}_i)}{V_E(\mathbf{u})}\,\mathbf{e}_i(\mathbf{u},\mathbf{x}).$$

□

Nous allons maintenant pouvoir calculer explicitement l'itération de Newton appliquée à $F_{\mathbf{f}}$. Pour cela, notons

$$\Delta_i\left(F_{\mathbf{f}}\right)(\mathbf{u}) = \frac{1}{V_E(\mathbf{u})}\begin{pmatrix} \partial_{x_1}(R_{f_1})(\mathbf{u},\mathbf{u}_i) & \cdots & \partial_{x_n}(R_{f_1})(\mathbf{u},\mathbf{u}_i) \\ \vdots & & \vdots \\ \partial_{x_1}(R_{f_n})(\mathbf{u},\mathbf{u}_i) & \cdots & \partial_{x_n}(R_{f_n})(\mathbf{u},\mathbf{u}_i) \end{pmatrix}.$$

***Théorème* 7.53.** *L'itération de Newton, appliquée au système $F_{\mathbf{f}}(\mathbf{u},\mathbf{x}) = 0$ est donnée, composante par composante, par*

$$\mathbf{u}'_i := \mathbf{u}_i - \Delta_i\left(F_{\mathbf{f}}\right)(\mathbf{u})^{-1}\begin{pmatrix} f_1(\mathbf{u}_i) \\ \vdots \\ f_n(\mathbf{u}_i) \end{pmatrix},\ i = 1,\ldots,D.$$

Démonstration. Calculons le vecteur $\mathtt{t} = (t_{i,j})_{1\le i\le n, 1\le j\le D}$ vérifiant

$$J_{F_{\mathbf{f}}}(\mathbf{u})\,\mathtt{t} = F_{\mathbf{f}},$$

et correspondant à la correction appliquée à $\mathbf{u}$ dans l'itération de Newton : $\mathbf{u}' = \mathbf{u} - \mathtt{t}$.

L'équation ci-dessus se traduit en terme de polynômes en $\mathbf{x}$ (obtenus en regroupant les coefficients par « paquets » de taille D) par

$$\sum_{i=1}^{n}\sum_{j=1}^{D}\partial_{u_{i,j}}(F_{f_k})(\mathbf{u},\mathbf{x})t_{i,j} = F_{f_k}(\mathbf{u},\mathbf{x}),\quad k = 1,\ldots,n.$$

D'après la proposition 7.52, nous déduisons pour tous $k = 1,\ldots,n, l = 1,\ldots,D$ que

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{D}\partial_{u_{i,j}}(F_{f_k})(\mathbf{u},\mathbf{u}_l)\,t_{i,j} - F_{f_k}(\mathbf{u},\mathbf{u}_l) &= 0\\ = \sum_{i=1}^{n}\sum_{j=1}^{D}\frac{1}{V_E(\mathbf{u})}\partial_{x_i}(R_{f_k})(\mathbf{u},\mathbf{u}_l)\,\mathbf{e}_j(\mathbf{u},\mathbf{u}_l)\,t_{i,j} - f_k(\mathbf{u}_l)&\\ = \sum_{i=1}^{n}\frac{1}{V_E(\mathbf{u})}\partial_{x_i}(R_{f_k})(\mathbf{u},\mathbf{u}_l)\,t_{i,l} - f_k(\mathbf{u}_l).&\end{aligned}$$

On a donc

$$\Delta_l(F_{\mathbf{f}})\begin{bmatrix} t_{1,l} \\ \vdots \\ t_{n,l} \end{bmatrix} = \begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix},$$

ou encore que

$$\mathtt{t}_l = (t_{1,l}, \ldots, t_{n,l}) = \Delta_l\left(F_{\mathbf{f}}\right)(\mathbf{u})^{-1} \begin{pmatrix} f_1(\mathbf{u}_l) \\ \vdots \\ f_n(\mathbf{u}_l) \end{pmatrix},$$

pour $l = 1, \ldots, D$. Ce qui achève la démonstration du théorème. □

Dans le cas d'une variable x et d'un polynôme f de degré d, nous avons

$$R_f(\mathbf{u}, \mathbf{x}) = \prod_{i<j}(u_i - u_j) \prod_{j=1}^{d}(x - u_j) = V_{1,\ldots,x^d}(\mathbf{u}) \prod_{j=1}^{d}(x - u_j)$$

et

$$\begin{aligned} \Delta_i(F_{\mathbf{f}})(\mathbf{u}) &= \frac{1}{V_{1,\ldots,x^d}(\mathbf{u})}\left[\partial_x(R_f)(u_i)\right] \\ &= \left[\partial_x\left(\prod_{j=1}^{d}(x - u_j)\right)(u_i)\right] = \left[\prod_{j\neq i}(u_i - u_j)\right]. \end{aligned}$$

Nous retrouvons donc bien l'itération de Weierstrass (7.14). Pour plus de détails, voir [**Rua01**] ou [**MR02**].

7.4. Exercices

***Exercice* 7.1.** Calculer une base de l'orthogonal de l'idéal $(x_1, \ldots, x_n)^2$.

***Exercice* 7.2.** Calculer la composante primaire à l'origine de

$$I = (x_1^2 - x_1\, x_2^2,\ x_1 + x_2^2).$$

***Exercice* 7.3.** Soit S la surface de $\mathbb{C}^3$ définie par $f(x, y, z) = x^2 - y^3 - y^2\, z^2$.

1. Calculer le système inverse $(0, 0, 0)$ de l'idéal I engendré par
$$f(x, y, z), \partial_x f(x, y, z), \partial_y f(x, y, z), \partial_z f(x, y, z).$$
2. Montrer que I contient une composante immergée en $(0, 0, 0)$.
3. Montrer que le système inverse en $(0, 0, 0)$ est engendré par un élément.

Pour une visualisation de cette surface ainsi que de son lieu singulier, voir la figure du chapitre suivant.

***Exercice* 7.4. Passage de l'homogène à l'affine.**

Soit $R_0 = \mathbb{K}[x_0, \ldots, x_n]$ l'anneau des polynômes en $n+1$ variables, à coefficients dans un corps $\mathbb{K}$ de caractéristique 0, et σ l'application

$$\begin{aligned} \sigma : R_0 &\to R \\ p(x_0, \ldots, x_n) &\mapsto p(1, x_1, \ldots, x_n). \end{aligned}$$

Rappelons les notations suivantes : $e^{\mathbf{d}_0} = \sum_{a\in\mathbb{N}} \mathbf{d}_0^a$, avec $\mathbf{d}_0^a(p) = \frac{\partial_{x_0}^a}{a!}(p)(0)$. Pour tout $\Lambda \in \widehat{R}_0$, nous notons $[\Lambda]_d$ la composante homogène de degré d de la série Λ.

1. Montrer que σ induit une application injective σ^* de $\widehat{R}$ dans $\widehat{R}_0$.
2. Soit J un idéal homogène de R_0 et $I = \sigma(J)$. Montrer que
$$\sigma_*(I^\perp) \subset J^\perp.$$
3. Montrer que l'image par l'application σ_* d'un élément $\mathbf{d}^m, m \in \mathbb{N}^n$, de la base duale des monômes est
$$\sigma_*(\mathbf{d}^m) = \mathbf{d}^m e^{\mathbf{d}_0}.$$
4. Notons $[\sigma_*(I^\perp)]_*$ le sous-espace vectoriel de $\widehat{R_0}$ engendré par toutes les composantes homogènes $[\Lambda]_d$ pour $\Lambda \in \sigma_*(I^\perp)$. Montrer que $[\sigma_*(I^\perp)]_*$ est stable par dérivation.
5. En déduire qu'il existe un unique idéal homogène $\tilde{J}$ dans R_0 tel que $\tilde{J}^\perp = [\sigma_*(I^\perp)]_*$.
6. En utilisant le fait que $\tilde{J}$ est homogène, montrer que $\tilde{J}^\perp \subset \sigma_*(I^\perp) \subset J^\perp$. En déduire que $J \subset \tilde{J}$.
7. Montrer que $\sigma(\tilde{J}) = I$.
8. Montrer que $(\tilde{J} : x_0) = \tilde{J}$.
9. Montrer que $\tilde{J}$ est le plus petit idéal de R_0 stable par division par x_0 et tel que $\sigma(\tilde{J}) = I$.
10. En déduire que pour tout idéal homogène J de R_0, on a
$$(J : x_0^*)^\perp = [e^{\mathbf{d}_0}\sigma(J)^\perp]_*$$
avec $(J : x_0^*) = \{p \in R; \exists N \in \mathbb{N},\ x_0^N p \in J\}$.

***Exercice* 7.5. Produit scalaire apolaire.** Soit $\mathbb{K}$ un corps de charactéristique 0 et $R = \mathbb{K}[x_1, \ldots, x_n]$. Dans cet exercice, pour $\alpha \in \mathbb{N}^n$ nous notons $\delta^\alpha = \delta^\alpha_{(0,\ldots,0)}$. Soit $R_{[d]}$ l'ensemble des polynômes de degré d de R, pour $d > 0$. Pour tout polynôme de la forme $p = \sum_\alpha p_\alpha \mathbf{x}^\alpha$, $(\alpha \in \mathbb{N}^n, p_\alpha \in \mathbb{K})$, on note $p(\delta) = \sum_\alpha p_\alpha \delta^\alpha$. Pour $p, q \in R_{[d]}$, notons $\langle p, q\rangle := p(\delta) \cdot q$.

1. Pour $\alpha, \beta \in \mathbb{N}^n$ avec $|\alpha| = |\beta| = d$, calculer $\langle \mathbf{x}^\alpha, \mathbf{x}^\beta\rangle$.
2. Montrer que l'application
$$(p, q) \mapsto \langle p, q\rangle := p(\delta) \cdot q$$
définit une forme bilinéaire symétrique non-dégénérée sur $R_{[d]}$. Ce produit scalaire est appelé *produit scalaire apolaire*. Nous notons $p^\perp = \{q \in R_{[d]}; \langle p, q\rangle = 0\}$. Si $q \in p^\perp$, on dira que p et q sont *apolaires*.
3. Pour $a = (a_1, \ldots, a_n) \in \mathbb{K}^n$, notons $l_a(\mathbf{x}) = a_1 x_1 + \cdots + a_n x_n$. Montrer que
$$\langle p, l_a^d\rangle = d!\, p(a)$$
4. Montrer que pour toute matrice $g \in \mathrm{Sl}_n(\mathbb{K})$, de déterminant 1, et pour tout $p, q \in R_{[d]}$ on a
$$\langle g \cdot p, g \cdot q\rangle = \langle p, q\rangle$$
où $g \cdot p(x_1, \ldots, x_n) = p(g \cdot (x_1, \ldots, x_n))$.

***Exercice* 7.6. Problème de Waring.** Nous reprenons les notations de l'exercice précédent. Nous allons nous intéresser au problème suivant :

Décomposer un polynôme de $R_{[d]}$ sous la forme

$$p = \lambda_1 \, l_{a_1}^d + \cdots + \lambda_r \, l_{a_r}^d,$$

avec $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$, $a_1, \ldots, a_r \in \mathbb{K}^n$ et r minimal.

1. Montrer que $p^\perp \supset \{q \in R_{[d]}; q(a_i) = 0, \text{ pour } i = 1, \ldots, r\}$.
2. Considérons l'application
$$\begin{array}{rcl} \phi_r : \mathbb{K}^n \times \cdots \times \mathbb{K}^n & \to & R_{[d]} \\ (a_1, \ldots, a_r) & \mapsto & l_{a_1}^d + \cdots + l_{a_r}^d. \end{array}$$
Nous notons $\overline{r}$ le plus petit r pour lequel l'adhérence $\overline{\mathrm{im}(\phi_r)} = R_{[d]}$. Montrer que $\overline{r}$ est le plus petit r tel que l'image de l'application différentielle $d\phi_r(a_1, \ldots, a_k)$ est $R_{[d]}$, pour $(a_1, \ldots, a_r)$ générique dans $\mathbb{K}^n \times \cdots \times \mathbb{K}^n$.
3. En déduire que $\overline{r}$ est le plus petit r pour lequel
$$x_1 l_{a_1}^{d-1}, \ldots, x_n l_{a_1}^{d-1}, \ldots, x_1 l_{a_r}^{d-1}, \ldots, x_n l_{a_r}^{d-1},$$
engendre $R_{[d]}$, pour $(a_1, \ldots, a_r)$ générique dans $\mathbb{K}^n \times \cdots \times \mathbb{K}^n$.
4. En déduire un algorithme probabiliste pour calculer $\overline{r}$.
5. Calculer $\overline{r}$ pour $n = 2, d = 2, 3, 4$, $n = 3, d = 2, 3, 4$, $n = 4, d = 2, 3, 4$, en utilisant cet algorithme.
6. Montrer que $p \in R_{[d]}$ vérifie
$$\langle p, x_1 l_a^{d-1} \rangle = \cdots = \langle p, x_n l_a^{d-1} \rangle = 0$$
si et seulement si $p(a) = \partial_1 p(a) = \cdots = \partial_n p(a) = 0$ (pour $a \in \mathbb{K}^n$).
7. En déduire que $\overline{r}$ est le plus petit r pour lequel il n'existe pas de polynôme $p \in R_{[d]}$ non-nul tel que p et ses dérivées $\partial_i p$ s'annulent en r points génériques $a_1, \ldots, a_r$ de $\mathbb{P}^{n-1}$.

***Exercice* 7.7. Sécantes de la variété de Veronese.** Nous reprenons les notations des deux exercices précédents et supposons de plus que $\mathbb{K}$ est algébriquement clos. Nous notons V_1 l'ensemble des polynômes non-nuls de $R_{[d]}$ de la forme l_a^d pour $a \in \mathbb{K}^n - \{\mathbf{0}\}$. Soit

$$V_r := S_r(V_1) := \{p \in R_{[d]};\ p = \mathbf{v}_1 + \cdots + \mathbf{v}_r, \text{ avec } \mathbf{v}_i \in V_1, i = 1, \ldots, r\}$$

et $\overline{V}_r$ son adhérence.

1. Montrer que V_1 est une variété algébrique projective (fermée) de $\mathbb{P}(R_{[d]})$.
2. Quelle est la dimension de V_1 ?
3. Calculer les équations de V_1 pour $n = 2, d = 2$.
4. Montrer que pour $d = 2$ et $n > 0$, V_1 est l'ensemble des formes quadratiques de rang 1.
5. Montrer que pour $d = 2$ et $n > 0$, V_r est l'ensemble des formes quadratiques de rang r.

6. Montrer que V_r est l'ensemble des points de $R_{[d]}$ sur des espaces linéaires engendrés par r points de V_1.
7. Calculer l'espace tangent en un point de V_r dans $R_{[d]}$.
8. Montrer que
   $$\mathrm{codim}(V_r) = \dim\{p \in R_{[d]}; p(a_i) = \partial_1 p(a_i) = \cdots = \partial_n p(a_i), i = 1, \ldots, n\},$$
   pour des points génériques $a_1, \ldots, a_r$ de $\mathbb{P}^{n-1}$.
9. Trouver un exemple de valeur de n et d pour lequel
   $$\dim(V_r) \neq \min\{n, r \times (n-1) + (r-1)\}.$$
10. Montrer que $V_{\overline{r}} = R_{[d]}$.