Polynômes en plusieurs indéterminées (commutatives)

Marc SAGE

29 octobre 2005 (màj mars 2018)

Table des matières

Soit A un anneau unitaire.

Nous généralisons ici la notion de polynôme à une indéterminée sur A – en somme $A[X]$ – au cas de plusieurs indéterminées indexées par un ensemble quelconque (non vide) – typiquement $\{1,...,n\}$, $\mathbb{N}$...

1 La A-algèbre $A\left[(X_i)_{i\in I}\right]$

Soit I un ensemble non vide, qui va servir à indexer nos indéterminées.

On sait qu'un polynôme à une indéterminée s'écrit

$$P=\sum_{\alpha\in\mathbb{N}}\lambda_\alpha X^\alpha$$

où les λ_α sont presque tous nuls.

Si on veut étendre ceci à des indéterminées $(X_i)_{i\in I}$, on posera naturellement

$$P=\sum_{\overrightarrow{\alpha}\in\mathbb{N}^I}\lambda_{\overrightarrow{\alpha}}\prod_{i\in I}X_i^{\alpha_i}$$

où $\lambda_{\overrightarrow{\alpha}}\in A$ est le coefficients de P associé au I-uplet $\overrightarrow{\alpha}$, avec les $\lambda_{\overrightarrow{\alpha}}$ à support fini.

Pour définit le produit $\prod_{i\in I}X_i^{\alpha_i}$, il faut que les $\overrightarrow{\alpha}$ soient presque tous nuls, ce qui s'écrit $\overrightarrow{\alpha}\in\mathbb{N}^{(I)}$.

Ainsi, P peut se définir à partir d'une famille $(\lambda_{\overrightarrow{\alpha}})\in A^{\left(\mathbb{N}^{(I)}\right)}$.

1.1 Définitions

Défintion.

*On appelle **polynôme** sur A (à indéterminées indexées par I) toute application de $\mathbb{N}^{(I)}$ dans A à support fini.*

On note

$$A\left[(X_i)_{i\in I}\right]:=A^{\left(\mathbb{N}^{(I)}\right)}$$

l'ensemble des polynômes sur A. On abrégera en $A[(X_i)]$ s'il n'y a pas ambiguïté sur l'ensemble I d'indexation.

On introduit également le I-uplet élémentaire correspondant à l'indice i tout seul

$$\overrightarrow{\varepsilon_i}:=\delta_{\cdot}^{i}\in\mathbb{N}^{(I)}$$

*ainsi que la i-ième **indéterminée***

$$X_i:=1_A\delta_{\cdot}^{\overrightarrow{\varepsilon_i}}\in A[(X_i)].$$

Proposition (structure de A-algèbre sur $A[(X_i)]$).

$A[(X_i)]$ est naturellement muni d'une structure de A-algèbre unitaire pour l'addition et la multiplication scalaire usuelles sur $A^{(?)}$ ainsi que le produit de Cauchy. Plus précisément :

$$\begin{cases} P+Q:=\begin{cases}\mathbb{N}^{(I)} & \longrightarrow & A\\ \overrightarrow{\alpha} & \longmapsto & P(\overrightarrow{\alpha})+Q(\overrightarrow{\alpha})\end{cases}\\ a\cdot P:=\begin{cases}\mathbb{N}^{(I)} & \longrightarrow & A\\ \overrightarrow{\alpha} & \longmapsto & aP(\overrightarrow{\alpha})\end{cases}\\ P\times Q:=\begin{cases}\mathbb{N}^{(I)} & \longrightarrow & A\\ \overrightarrow{\alpha} & \longmapsto & \sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{\alpha}}P(\overrightarrow{u})\,Q(\overrightarrow{v})\end{cases}\\ 1_{A[(X_i)]}:=1_A\delta_{\cdot}^{\overrightarrow{0}}\end{cases}.$$

D'autre part, si $P_1,...,P_n$ sont $n\geq 1$ polynômes dans $A[(X_i)]$, on a

$$P_1...P_n(\overrightarrow{\alpha})=\sum_{\overrightarrow{u_1}+...+\overrightarrow{u_n}=\overrightarrow{\alpha}}P_1(\overrightarrow{u_1})...P_n(\overrightarrow{u_n})$$

Démonstration.

Il est clair que + est associative, commutative, et admet l'élément neutre $\left\{\begin{array}{ccc}\mathbb{N}^{(I)} & \longrightarrow & A \\ \overrightarrow{u} & \longmapsto & 0\end{array}\right.$.

De plus, on a facilement la distributivité de $\cdot$ sur + :

$$\begin{aligned}[(a+b)\cdot(P+Q)](\overrightarrow{\alpha}) &= (a+b)[P+Q](\overrightarrow{\alpha}) \\ &= (a+b)(P(\overrightarrow{\alpha})+Q(\overrightarrow{\alpha})) \\ &= aP(\overrightarrow{\alpha})+aQ(\overrightarrow{\alpha})+bP(\overrightarrow{\alpha})+bQ(\overrightarrow{\alpha}) \\ &= [a\cdot P](\overrightarrow{\alpha})+[a\cdot Q](\overrightarrow{\alpha})+[b\cdot P](\overrightarrow{\alpha})+[b\cdot Q](\overrightarrow{\alpha}) \\ &= [a\cdot P+a\cdot Q+b\cdot P+b\cdot Q](\overrightarrow{\alpha}).\end{aligned}$$

On vérifie enfin que

$$[1_A\cdot P](\overrightarrow{\alpha}) = 1_A P(\overrightarrow{\alpha}) = P(\overrightarrow{\alpha}).$$

Ainsi, $A[(X_i)]$ est un A-module pour les lois + et $\cdot$.

La somme $\sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{\alpha}}$ définissant le produit est bien finie car $\overrightarrow{\alpha}$ est à support fini et à valeurs dans $\mathbb{N}$, donc chacune des coordonnées α_i de $\overrightarrow{\alpha}$ ne peut se décomposer que d'un nombre fini de façons

Il est moins clair que $\times$ est associative. On calcule de deux manières :

$$\begin{aligned}[(P\times Q)\times R](\overrightarrow{\alpha}) &= \sum_{\overrightarrow{\beta}+\overrightarrow{w}=\overrightarrow{\alpha}}[P\times Q]\left(\overrightarrow{\beta}\right)R(\overrightarrow{w}) \\ &= \sum_{\overrightarrow{\beta}+\overrightarrow{w}=\overrightarrow{\alpha}}\left(\sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{\beta}}P(\overrightarrow{u})Q(\overrightarrow{v})\right)R(\overrightarrow{w}) \\ &= \sum_{\overrightarrow{u}+\overrightarrow{v}+\overrightarrow{w}=\overrightarrow{\alpha}}P(\overrightarrow{u})Q(\overrightarrow{v})R(\overrightarrow{w})\end{aligned}$$

et

$$\begin{aligned}[P\times(Q\times R)](\overrightarrow{\alpha}) &= \sum_{\overrightarrow{u}+\overrightarrow{\beta}=\overrightarrow{\alpha}}P(\overrightarrow{u})[Q\times R]\left(\overrightarrow{\beta}\right) \\ &= \sum_{\overrightarrow{u}+\overrightarrow{\beta}=\overrightarrow{\alpha}}P(\overrightarrow{u})\left(\sum_{\overrightarrow{v}+\overrightarrow{w}=\overrightarrow{\beta}}Q(\overrightarrow{v})R(\overrightarrow{w})\right) \\ &= \sum_{\overrightarrow{u}+\overrightarrow{v}+\overrightarrow{w}=\overrightarrow{\alpha}}P(\overrightarrow{u})Q(\overrightarrow{v})R(\overrightarrow{w}).\end{aligned}$$

Reste à vérifier la distributivité de $\times$ sur + :

$$\begin{aligned}[P(A+B)](\overrightarrow{\alpha}) &= \sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{a}}P(\overrightarrow{u})[A+B](\overrightarrow{v}) \\ &= \sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{a}}P(\overrightarrow{u})(A(\overrightarrow{v})+B(\overrightarrow{v})) \\ &= \sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{a}}P(\overrightarrow{u})A(\overrightarrow{v})+\sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{a}}P(\overrightarrow{u})B(\overrightarrow{v}) \\ &= PA(\overrightarrow{\alpha})+PB(\overrightarrow{\alpha})\end{aligned}$$

et exactement pareil à droite.

Enfin, on s'assure que $1_A\delta_{\cdot}^{\overrightarrow{0}}$ est bien le neutre pour $\times$:

$$\left[\left(1_A\delta_{\cdot}^{\overrightarrow{0}}\right)\times P\right](\overrightarrow{u}) = \sum_{\overrightarrow{v}+\overrightarrow{w}=\overrightarrow{u}}1_A\delta_{\overrightarrow{v}}^{\overrightarrow{0}}P(\overrightarrow{w}) = P(\overrightarrow{u}).$$

$A[(X_i)]$ est donc un anneau pour les lois + et $\times$.

Montrons que ces deux structures sont compatibles. Soient P, Q deux polynômes et $a \in A$. Alors

$$\begin{aligned}
[P \times (a \cdot Q)](\overrightarrow{\alpha}) &= \sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{\alpha}} P(\overrightarrow{u})[a \cdot Q](\overrightarrow{v}) \\
&= \sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{\alpha}} P(\overrightarrow{u})\, aQ(\overrightarrow{v}) \\
&= a \sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{\alpha}} P(\overrightarrow{u})\, Q(\overrightarrow{v}) \\
&= a\,[P \times Q](\overrightarrow{\alpha}),
\end{aligned}$$

et idem pour $[(a \cdot P) \times Q](\overrightarrow{\alpha})$.

On montre ensuite par récurrence la formule donnant le produit $P_1 ... P_n$. Pour $n = 1$, la formule est tautologique. Pour $n = 2$, c'est la définition du produit. Pour $n \geq 3$, on écrit

$$\begin{aligned}
P_1 ... P_n(\overrightarrow{\alpha}) &= [(P_1 ... P_{n-1}) P_n](\overrightarrow{\alpha}) \\
&= \sum_{\overrightarrow{\beta}+\overrightarrow{u_n}=\overrightarrow{\alpha}} [P_1 ... P_{n-1}]\left(\overrightarrow{\beta}\right) P_n(\overrightarrow{u_n}) \\
&= \sum_{\overrightarrow{\beta}+\overrightarrow{u_n}=\overrightarrow{\alpha}} \ \sum_{\overrightarrow{u_1}+...+\overrightarrow{u_{n-1}}=\overrightarrow{\beta}} P_1(\overrightarrow{u_1}) ... P_{n-1}(\overrightarrow{u_{n-1}}) P_n(\overrightarrow{u_n}) \\
&= \sum_{\overrightarrow{u_1}+...+\overrightarrow{u_n}=\alpha} P_1(\overrightarrow{u_1}) ... P_n(\overrightarrow{u_n}).
\end{aligned}$$

1.2 Écriture canonique des polynômes

Proposition (commutativité des indéterminées).
Les indéterminées X_i commutent deux à deux, de sorte que le produit

$$\prod_{i \in I} X_i^{\alpha_i}$$

fait sens pour chaque $\overrightarrow{\alpha} \in \mathbb{N}^{(I)}$. On a plus précisémenent

$$\prod_{i \in I} X_i^{\alpha_i} = \delta_{\cdot}^{\overrightarrow{\alpha}}.$$

Démonstration.
Il suffit d'écrire

$$X_i X_j(\overrightarrow{\alpha}) = \sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{\alpha}} X_i(\overrightarrow{u}) X_j(\overrightarrow{v}) = \sum_{\overrightarrow{u}+\overrightarrow{v}=\overrightarrow{\alpha}} \delta_{\overrightarrow{u}}^{\overrightarrow{\varepsilon_i}} \delta_{\overrightarrow{v}}^{\overrightarrow{\varepsilon_j}} = \delta_{\overrightarrow{\alpha}}^{\overrightarrow{\varepsilon_i}+\overrightarrow{\varepsilon_j}}$$

qui est indépendant de l'ordre entre i et j.
Ensuite, on note que pour $n \geq 1$ on a

$$X_i^n(\overrightarrow{u}) = \sum_{\overrightarrow{u_1}+...+\overrightarrow{u_n}=\overrightarrow{\alpha}} X_i(\overrightarrow{u_1}) ... X_i(\overrightarrow{u_n}) = \sum_{\overrightarrow{u_1}+...+\overrightarrow{u_n}=\overrightarrow{u}} \delta_{\overrightarrow{u_1}}^{\overrightarrow{\varepsilon_i}} ... \delta_{\overrightarrow{u_n}}^{\overrightarrow{\varepsilon_i}} = \delta_{\overrightarrow{u}}^{n\overrightarrow{\varepsilon_i}}.$$

On peut ainsi calculer

$$\left[\prod_{i \in I} X_i^{\alpha_i}\right](\overrightarrow{u}) = \sum_{\sum_{i \in I}^{\alpha_i \neq 0} \overrightarrow{v_i}=\overrightarrow{u}} \ \prod_{i \in I} X_i^{\alpha_i}(\overrightarrow{v_i}) = \sum_{\sum_{i \in I}^{\alpha_i \neq 0} \overrightarrow{v_i}=\overrightarrow{u}} \ \prod_{i \in I} \delta_{\overrightarrow{v_i}}^{\alpha_i \overrightarrow{\varepsilon_i}} = \delta_{\overrightarrow{u}}^{\sum_{i \in I}^{\alpha_i \neq 0} \alpha_i \overrightarrow{\varepsilon_i}} = \delta_{\overrightarrow{u}}^{\overrightarrow{\alpha}}.$$

Corollaire (écriture canonique des polynômes).

Chaque polynôme P de $A[(X_i)]$ s'écrit de façon unique sous la forme

$$P = \sum_{\overrightarrow{\alpha} \in \mathbb{N}^{(I)}} \lambda_{\overrightarrow{\alpha}} \prod_{i \in I} X_i^{\alpha_i}$$

où les $\lambda_{\overrightarrow{\alpha}} \in A$ sont à support fini. On a en fait

$$\lambda_{\overrightarrow{\alpha}} = P(\overrightarrow{\alpha}) \text{ pour chaque } \overrightarrow{\alpha} \in \mathbb{N}^{(I)}.$$

Démonstration.
Il suffit d'écrire

$$\left[\sum_{\overrightarrow{\alpha} \in \mathbb{N}^{(I)}} P(\overrightarrow{\alpha}) \prod_{i \in I} X_i^{\alpha_i} \right] (\overrightarrow{u}) = \sum_{\overrightarrow{\alpha} \in \mathbb{N}^{(I)}} P(\overrightarrow{\alpha}) \left[\prod_{i \in I} X_i^{\alpha_i} \right] (\overrightarrow{u}) = \sum_{\overrightarrow{\alpha} \in \mathbb{N}^{(I)}} P(\overrightarrow{\alpha}) \delta_{\overrightarrow{u}}^{\overrightarrow{\alpha}} = P(\overrightarrow{u}),$$

d'où l'existence en posant $\lambda_{\overrightarrow{\alpha}} = P(\overrightarrow{\alpha})$.
Concernant l'unicité, si on a une décomposition

$$P = \sum_{\overrightarrow{\alpha} \in \mathbb{N}^{(I)}} \lambda_{\overrightarrow{\alpha}} \prod_{i \in I} X_i^{\alpha_i},$$

le calcul ci-dessus montre que nécessairement $\lambda_{\overrightarrow{\alpha}} = P(\overrightarrow{\alpha})$ pour chaque $\overrightarrow{\alpha}$.

Remarques. Vue l'égalité "indicielle" $\lambda_{\overrightarrow{\alpha}} = P(\overrightarrow{\alpha})$, on laissera de côté la notation fonctionnelle de P : son $\overrightarrow{\alpha}$-ième coefficient sera désormais noté $[P]_{\overrightarrow{\alpha}}$, à l'instar de l'écriture matricielle.

Usuellement, on note $\overrightarrow{X} = (X_i)_{i \in I}$, et on laisse même tomber toutes les flèches. La forme ci-dessus s'écrit alors

$$P = \sum_{\alpha \in \mathbb{N}^{(I)}} \lambda_\alpha X^\alpha, \text{ voire } \sum \lambda_\alpha X^\alpha$$

où les λ_a sont presque tous nuls.

On dispose alors de la propriété fondamentale

$$\left[\sum \lambda_\alpha X^\alpha = \sum \mu_\alpha X^\alpha \right] \iff [\forall \alpha,\ \lambda_\alpha = \mu_\alpha].$$

En outre, pour un produit de $n \geq 1$ polynômes, on a l'identité

$$P_1 ... P_n = \sum_{\overrightarrow{\alpha}} \left(\sum_{\overrightarrow{u_1} + ... + \overrightarrow{u_n} = \overrightarrow{\alpha}} [P_1]_{\overrightarrow{u_1}} ... [P_n]_{\overrightarrow{u_n}} \right) X^\alpha$$

(remplacer $[P_1 ... P_n]_{\overrightarrow{\alpha}}$ par sa valeur calculée précédemment).

Plus précisément, on a :

$$\begin{aligned} \left(\sum \lambda_\alpha^{(1)} X^\alpha \right) ... \left(\sum \lambda_\alpha^{(n)} X^\alpha \right) &= \sum_{\overrightarrow{u_1}, ..., \overrightarrow{u_n}} \lambda_{\overrightarrow{u_1}}^{(1)} ... \lambda_{\overrightarrow{u_n}}^{(n)} X^{\overrightarrow{u_1} + ... + \overrightarrow{u_n}} \text{ par multidistributivité} \\ &= \sum_{\overrightarrow{\alpha}} \left(\sum_{\overrightarrow{u_1} + ... + \overrightarrow{u_n} = \overrightarrow{\alpha}} \lambda_{\overrightarrow{u_1}}^{(1)} ... \lambda_{\overrightarrow{u_n}}^{(n)} \right) X^\alpha \text{ en regroupant les termes.} \end{aligned}$$

On notera que, si A est commutatif, on a

$$\sum_\alpha \lambda_\alpha X^\alpha \sum_\beta \mu_\beta X^\beta = \sum_{\alpha, \beta} \lambda_\alpha \mu_\beta X^{\alpha + \beta} = \sum_{\alpha, \beta} \mu_\beta \lambda_\alpha X^{\beta + a} = \sum_\beta \mu_\beta X^\beta \sum_\alpha \lambda_\alpha X^\alpha$$

et donc $A[(X_i)]$ est commutative.

Le passage de l'intégrité est plus délicat et utilise les isomorphismes usuels exposés en seconde partie.

2 Isomorphismes usuels

2.1 Injection de A dans $A\left[(X_i)_{i\in I}\right]$

Proposition.
L'anneau A (considéré comme A-algèbre) se plonge canoniquement dans l'algèbre $A[(X_i)]$ via

$$\left\{\begin{array}{ccc} A & \hookrightarrow & A[(X_i)] \\ a & \longmapsto & a\mathbf{1} \end{array}\right.$$

où l'on a noté $\mathbf{1}$ le neutre de $A[(X_i)]$ par commodité.

Démonstration. Notons ι l'application considérée.
L'injectivité s'obtient en écrivant

$$\iota(a)=\iota(b) \implies [a\mathbf{1}]_{\overrightarrow{0}}=[b\mathbf{1}]_{\overrightarrow{0}} \implies a=b,$$

le caractère "morphique" de ι découle de

$$\begin{array}{rcl} \iota(ab+c) & = & (ab+c)\,\mathbf{1} \\ & = & ab\mathbf{1}+c\mathbf{1} \\ & = & (a\mathbf{1})(b\mathbf{1})+(c\mathbf{1}) \\ & = & \iota(a)\,\iota(b)+\iota(c)\,, \end{array}$$

de

$$\iota(a\cdot x)=\iota(a\times x)=\iota(a)\times\iota(x)=a\mathbf{1}\times\iota(x)=a\cdot\iota(x)$$

et de

$$\iota(1_A)=1_A\mathbf{1}=\mathbf{1}.$$

2.2 Injection de $A[(X_i)]$ dans $B[(X_i)]$ si $A\hookrightarrow B$

Proposition.
Soient $\varphi : A\hookrightarrow B$ un morphisme injectif d'anneaux unitaires.
Alors la A-algèbre $A[(X_i)]$ s'injecte canoniquement dans la B-algèbre $B[(X_i)]$ par

$$\left\{\begin{array}{ccc} A[(X_i)] & \hookrightarrow & B[(X_i)] \\ \sum\lambda_\alpha X^\alpha & \longmapsto & \sum\boldsymbol{\lambda}_\alpha X^\alpha \end{array}\right. .\text{où } \boldsymbol{\lambda} \text{ abrège } \varphi(\lambda) \text{ pour chaque } \lambda\in A.$$

Démonstration. Notons Φ l'application considérée.
Pour trois polynômes P,Q,R, on peut toujours écrire

$$\begin{array}{rcl} aPQ+R & = & \left(a\sum_\alpha\lambda_\alpha X^\alpha\right)\left(\sum_\beta\mu_\beta X^\beta\right)+\sum_\gamma\nu_\gamma X^\gamma \\ & = & \sum_\gamma a\left(\sum_{\alpha+\beta=\gamma}\lambda_\alpha\mu_\beta\right)X^\gamma+\sum_\gamma\nu_\gamma X^\gamma \\ & = & \sum_\gamma\left(\nu_\gamma+a\sum_{\alpha+\beta=\gamma}\lambda_\alpha\mu_\beta\right)X^\gamma. \end{array}$$

En appliquant Φ, en utilisant que φ est un morphisme d'anneaux, puis en remontant le calcul ci-dessus, on voit que Φ est un morphisme d'algèbres.
L'injectivité découle de celle de φ.

Applications. Le cas le plus courant est celui de l'inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$, qui permet de voir un polynôme réel dans $\mathbb{C}$ afin de le scinder. Par exemple, soit A une matrice réelle nilpotente. Son polynôme caractéristique peut ne pas avoir de racines, à l'instar de $\chi\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = X^2 + 1$, mais en le plongeant dans $\mathbb{C}$ on lui trouve n racines λ_i, lesquelle doivent toutes vérifier $\lambda_i^n = 0$ en itérant par A suffisamment de fois. Ceci montre que toutes les racines de χ_A dans $\mathbb{C}$ sont nulles, d'où $\chi_A = X^n$ dans $\mathbb{C}[X]$, donc dans $\mathbb{R}[X]$ par injectivité du plongement $\mathbb{R}[X] \hookrightarrow \mathbb{C}[X]$. Évidemment, ce raisonnement fonctionne en plongeant un corps quelconque dans sa clôture algébrique.

On utilisera également cette injection pour montrer que deux matrices de $M_n(k)$ semblables dans une extension $k \hookrightarrow K$ sont en fait semblables dans le petit corps : voir le cours sur les invariants de similitudes.

Il peut également être intéressant de plonger un anneau intègre dans son corps des fractions, à l'instar de $\mathbb{Z} \hookrightarrow \mathbb{Q}$. En effet, l'étude des irréductibles de $\mathbb{Z}[X]$ passe par celle des irréductibles de $\mathbb{Q}[X]$.

Corollaire.
Soient A et A' deux anneaux unitaires isomorphes, mettons $A \overset{\varphi}{\simeq} A'$.
Alors la A-algèbre $A[(X_i)]$ et la A'-algèbre $A'[(X_i)]$ sont canoniquement isomorphes via

$$\left\{\begin{array}{ccc} A[(X_i)] & \simeq & B[(X_i)] \\ \sum \lambda_\alpha X^\alpha & \longmapsto & \sum \lambda'_\alpha X^\alpha \end{array}\right. \quad \text{où } \lambda' := \varphi(\lambda) \text{ pour chaque } \lambda \in A.$$

2.3 Permtutation des indéterminées

Proposition (permutation des indéterminées).
Soient I et J deux ensembles non vides. On note $I \sqcup J$ leur réunion disjointe.

On notera par commodité (Y_j) les indéterminées de $A\left[(X_j)_{j\in J}\right]$ et (Z_k) les indéterminées de $A\left[(X_k)_{k\in I\sqcup J}\right]$.

Alors les A-algèbres $A[(X_i)][(Y_j)]$ et $A[(Y_j)][(X_i)]$ sont tous deux isomorphes à $A[(Z_k)]$ par l'application canonique

$$\left\{\begin{array}{ccc} A[(Y_j)][(X_i)] & \simeq & A[(Z_k)] \\ P & \longmapsto & \sum_{\beta\in\mathbb{N}^{(J)}}^{\alpha\in\mathbb{N}^{(I)}} [[P]_\alpha]_\beta X^\alpha Y^\beta \end{array}\right. .$$

Démonstration. Notons Φ l'application considéréen, soient P et Q dans $A[(Y_j)][(X_i)]$.
Concernant la linéarité, tout se passe bien :

$$\begin{aligned}
\Phi(aP + Q) &= \sum_{\alpha,\beta} [[aP + Q]_\alpha]_\beta X^\alpha Y^\beta \\
&= \sum_{\alpha,\beta} [a[P]_\alpha + [Q]_\alpha]_\beta X^\alpha Y^\beta \\
&= \sum_{\alpha,\beta} \left(a[[P]_\alpha]_\beta + [[Q]_\alpha]_\beta\right) X^\alpha Y^\beta \\
&= \sum_{\alpha,\beta} a[[P]_\alpha]_\beta X^\alpha Y^\beta + \sum_{\alpha,\beta} [[Q]_\alpha]_\beta X^\alpha Y^\beta \\
&= a\Phi(P) + \Phi(Q).
\end{aligned}$$

Pour le produit, on s'y prend en deux fois :

$$\begin{aligned}
\Phi(PQ) &= \sum_{\alpha,\beta} [[PQ]_\alpha]_\beta X^\alpha Y^\beta \\
&= \sum_{\alpha,\beta} \sum_{\alpha'+\alpha''=\alpha} [[P]_{\alpha'} [Q]_{\alpha''}]_\beta X^\alpha Y^\beta \\
&= \sum_{\alpha,\beta} \sum_{\alpha'+\alpha''=\alpha} \sum_{\beta'+\beta''=\beta} \left([[P]_{\alpha'}]_{\beta'} \times [[Q]_{\alpha''}]_{\beta''}\right) X^\alpha Y^\beta
\end{aligned}$$

et

$$\begin{aligned}
\Phi(P)\,\Phi(Q) &= \sum_{\alpha',\beta'} [[P]_{\alpha'}]_{\beta'} X^{\alpha'} Y^{\beta'} \sum_{\alpha'',\beta''} [[Q]_{\alpha''}]_{\beta''} X^{\alpha''} Y^{\beta''} \\
&= \sum_{\alpha',\alpha''\beta',\beta''} [[P]_{\alpha'}]_{\beta'} \times [[Q]_{\alpha''}]_{\beta''} X^{\alpha'+\alpha''} Y^{\beta'+\beta''} \\
&= \sum_{\alpha,\beta} \sum_{\substack{\alpha'+\alpha''=\alpha \\ \beta'+\beta''=\beta}} [[P]_{\alpha'}]_{\beta'} \times [[Q]_{\alpha''}]_{\beta''} X^{\alpha'+\alpha''} Y^{\beta'+\beta''} \\
&= \sum_{\alpha,\beta} \sum_{\alpha'+\alpha''=\alpha} \sum_{\beta'+\beta''=\beta} \left([[P]_{\alpha'}]_{\beta'} \times [[Q]_{\alpha''}]_{\beta''}\right) X^{\alpha} Y^{\beta}.
\end{aligned}$$

Montrons maintenant l'injectivité :

$$\begin{aligned}
\Phi(P) = 0 \quad &\Longrightarrow \quad \sum_{\alpha,\beta\in\mathbb{N}^{(I)}\times\mathbb{N}^{(J)}} [[P]_{\alpha}]_{\beta} X^{\alpha} Y^{\beta} = 0 \\
&\Longrightarrow \quad \forall\alpha \in \mathbb{N}^{(I)},\ \forall\beta \in \mathbb{N}^{(J)},\ [[P]_{\alpha}]_{\beta} = 0 \\
&\Longrightarrow \quad \forall\alpha \in \mathbb{N}^{(I)},\ [P]_{\alpha} = 0 \\
&\Longrightarrow \quad P = 0.
\end{aligned}$$

Enfin, pour la surjectivité, il suffit de noter que $\mathbb{N}^{(I\sqcup J)}$ est en bijection avec $\mathbb{N}^{(I)} \times \mathbb{N}^{(J)}$ via

$$\gamma \longmapsto \left(\gamma_{|I}, \gamma_{|J}\right).$$

Ainsi, chaque $R \in A[(Z_k)]$ s'écrit

$$R = \sum_{\gamma\in\mathbb{N}^{(I\sqcup J)}} \lambda_\gamma Z^\gamma = \sum_{\gamma\in\mathbb{N}^{(I\sqcup J)}} \lambda_\gamma X^{\gamma_{|I}} Y^{\gamma_{|J}} = \sum_{\substack{\alpha\in\mathbb{N}^{(I)} \\ \beta\in\mathbb{N}^{(J)}}} \lambda_{\alpha,\beta} X^\alpha Y^\beta = \Phi\left(\sum_{\alpha\in\mathbb{N}^{(I)}} \left(\sum_{\beta\in\mathbb{N}^{(J)}} \lambda_{\alpha,\beta} Y^\beta\right) X^\alpha\right).$$

Ceci conclut les vérifications.

On notera par conséquent indifféremment

$$\begin{gathered}
\sum_{\alpha} \left(\sum_{\beta} \lambda_{\alpha,\beta} Y^\beta\right) X^\alpha \\
\sum_{\alpha} \sum_{\beta} \lambda_{\alpha,\beta} Y^\beta X^\alpha \\
\sum_{\alpha,\beta} \lambda_{\alpha,\beta} X^\alpha Y^\beta \\
\sum_{\beta} \sum_{\alpha} \lambda_{\alpha,\beta} X^\alpha Y^\beta \\
\sum_{\beta} \left(\sum_{\alpha} \lambda_{\alpha,\beta} X^\alpha\right) Y^\beta
\end{gathered}$$

selon que l'on considère le polynôme dans $A[(X_i)]$, $A[(Y_j)]$ ou $A[(Z_k)]$.

2.4 Réindextation des indéterminées

Proposition (réindexation des indéterminées).
Soit J un ensemble en bijection avec I, disons $J = \varphi(I)$.

Alors les A-algèbres $A\left[(X_i)_{i\in I}\right]$ et $A\left[(X_j)_{j\in J}\right]$ sont canoniquement isomorphes par

$$\left\{\begin{array}{ccc} A\left[(X_j)_{j\in J}\right] & \longrightarrow & A\left[(X_i)_{i\in I}\right] \\ \sum_{\alpha\in\mathbb{N}^{(J)}}\lambda_\alpha X^\alpha & \longmapsto & \sum_{\alpha\in\mathbb{N}^{(J)}}\lambda_\alpha X^{\alpha\circ\varphi} \end{array}\right. \quad \text{où l'on a noté } X^{\alpha\circ\varphi} := \prod_{i\in I} X_i^{\alpha_{\varphi(i)}}.$$

Démonstration. Notons Φ l'application considérée. Comme toujours, on y va la tête haute...
La linéarité :

$$\begin{aligned} \Phi(aP+Q) &= \sum_\alpha [aP+Q]_\alpha X^{\alpha\circ\varphi} \\ &= \sum_\alpha \left(a[P]_\alpha + [Q]_\alpha\right) X^{\alpha\circ\varphi} \\ &= \sum_\alpha a[P]_\alpha X^{\alpha\circ\varphi} + \sum_\alpha [Q]_\alpha X^{\alpha\circ\varphi} \\ &= a\Phi(P) + \Phi(Q). \end{aligned}$$

La multiplicativité :

$$\begin{aligned} \Phi(PQ) &= \sum_\alpha [PQ]_\alpha X^{\alpha\circ\varphi} \\ &= \sum_\alpha \sum_{u+v=\alpha} [P]_u [Q]_v X^{\alpha\circ\varphi} \\ &= \sum_\alpha \sum_{u+v=\alpha} [P]_u [Q]_v X^{(u+v)\circ\varphi} \\ &= \sum_\alpha \sum_{u+v=\alpha} [P]_u [Q]_v X^{u\circ\varphi} X^{v\circ\varphi} \\ &= \sum_u [P]_u X^{u\circ\varphi} \sum_v [Q]_v X^{v\circ\varphi} \\ &= \Phi(P)\Phi(Q). \end{aligned}$$

L'unitarité :

$$\Phi(1) = 1X^{\overrightarrow{0}\circ\varphi} = \prod_{i\in I} X_i^{\overrightarrow{0}_{\varphi(i)}} = \prod_{i\in I} X_i^0 = \prod_{i\in I}\mathbf{1} = \mathbf{1}.$$

Pour obtenir l'injectivité, il faut tout d'abord remarquer que les $X^{\alpha\circ\varphi}$ sont distincts quand α varie dans $\mathbb{N}^{(J)}$:

$$\begin{aligned} X^{\alpha\circ\varphi} = X^{\alpha'\circ\varphi} &\Longrightarrow \prod_{i\in I} X_i^{\alpha_{\varphi(i)}} = \prod_{i\in I} X_i^{\alpha'_{\varphi(i)}} \\ &\Longrightarrow \forall i\in I,\ \alpha_{\varphi(i)} = \alpha'_{\varphi(i)} \\ &\Longrightarrow \forall j\in J,\ \alpha_{\varphi(\varphi^{-1}(j))} = \alpha'_{\varphi(\varphi^{-1}(j))} \\ &\Longrightarrow \forall j\in J,\ \alpha_j = \alpha'_j \\ &\Longrightarrow \overrightarrow{\alpha} = \overrightarrow{\alpha'}. \end{aligned}$$

Ainsi,

$$\begin{aligned} \Phi(P) = 0 &\Longrightarrow \sum_\alpha [P]_a X^{\alpha\circ\varphi} = 0 \\ &\Longrightarrow \forall\alpha\in\mathbb{N}^{(J)},\ [P]_\alpha = 0 \\ &\Longrightarrow P = 0. \end{aligned}$$

La surjectivité découle de

$$\sum_{\alpha\in\mathbb{N}^{(I)}} \lambda_\alpha X^\alpha = \sum_{\alpha\in\mathbb{N}^{(J)}} \lambda_{\alpha\circ\varphi^{-1}} X^{\alpha\circ\varphi^{-1}} = \Phi\left(\sum_{\alpha\in\mathbb{N}^{(J)}} \lambda_{\alpha\circ\varphi^{-1}} X^\alpha\right).$$

La dernière proposition nous dit que l'on peut se ramener au cas où I est un ensemble de référence de cardinal fixé. On prend naturellement la "suite" des cardinaux $(\aleph_\alpha)$ indexée par les ordinaux.

Par exemple, lorsque I est fini de cardinal $n \geq 1$, on prend comme ensemble de rérérérence le n-ième cardinal $\underline{n}= \{\underline{0}, ..., \underline{n-1}\}$. Alors[1] $\mathbb{N}^{(I)} = \mathbb{N}^I = \mathbb{N}^{\underline{n}}$, donc chaque polynôme P de $A[X_1, ..., X_n]$ s'écrit

$$P = \sum_{(\alpha_1,...,\alpha_n)\in\mathbb{N}^n} \lambda_{\alpha_1,...,\alpha_n} X_1^{\alpha_1}...X_n^{\alpha_n} \text{ où les } \lambda_{\alpha_1,...,\alpha_n} \text{ sont à support fini.}$$

Ces quatre isomorphismes – par ailleurs complètement naturels, il faut s'en convaincre – étant acquis, on peut passer à l'intégrité de $A[(X_i)]$.

2.5 Intégrité de $A[(X_i)]$ si A intègre

A s'injectant dans $A[(X_i)]$, une condition nécessaire pour avoir l'intégrité de $A[(X_i)]$ est évidemment que A soit intègre. La réciproque se trouve être vraie.

Proposition.
Si A est intègre, alors l'algèbre $A[(X_i)]$ est intègre.

Démonstration.
On part d'une relation $PQ = 0$ où P et Q sont des polynômes. Regroupons les indéterminées X_j qui apparaissent dans P et Q, lesquelles sont en nombre fini, et notons J le sous-ensemble fini de I qui les indexe. L'égalité $PQ = 0$ peut donc se voir dans $A\left[(X_j)_{j\in J}\right]$ en remontant les injections

$$A\left[(X_j)_{j\in J}\right] \hookrightarrow A\left[(X_j)_{j\in J}\right]\left[(X_k)_{k\in I\setminus J}\right] \overset{\text{permutation}}{\simeq} A\left[(X_l)_{l\in J\sqcup I\setminus J}\right] \overset{\text{réindextation}}{\simeq} A\left[(X_i)_{i\in I}\right].$$

On est donc ramené au cas où I fini. De plus, vu l'isomorphisme

$$A[X_1, ..., X_n][X_{n+1}] \simeq A[X_1, ..., X_{n+1}],$$

il suffit de regarder le cas où I est réduit à un élément.

Notons X l'indéterminée correspondante. Dans l'égalité $PQ = 0$, si $P = \sum_{i=0}^p p_i X^i$ et $Q = \sum_{j=0}^q q_j X^j$ sont non nuls, leurs degrés p et q sont ≥ 0, d'où

$$0 = [PQ]_{p+q} = \sum_{i+j=p+q} P(i)\,Q(j) = P(p)\,Q(q) \neq 0, \text{ contradiction.}$$

3 Fonctions polynomiales – Morphisme d'évalutation

On considère $\mathcal{A}$ une A-algèbre unitaire. Rappelons que cela induit un morphisme d'anneaux

$$\iota := \left\{ \begin{array}{ccc} A & \longrightarrow & \mathcal{A} \\ a & \longmapsto & a \times 1_{\mathcal{A}} \end{array} \right. .$$

Si $\mathcal{A}$ est une algèbre non nulle sur un corps, par exemple $\mathcal{A} = M_n(K)$ ou $\mathcal{A} = K[X]$, il est facile de voir que ι est injectif (d'où la notation ι).

[1] On notera un léger abus de notations : le produit cartésien étant défini comme un espace de fonctions, par exemple $\mathbb{N}^n := \mathbb{N}^{\underline{n}}$, l'ensemble $\mathbb{N}^1$ n'est pas ensemblistement égal à $\mathbb{N}$, bien que l'on dispose d'une bijection évidente.

Mais cela est faux en général : considérer un anneau A non intègre, disons $ab = 0$ avec a et b non nuls, et $\mathcal{A}$ une algèbre de neutre a, par exemple $\mathcal{A} = {}^{A}\!\big/_{1-a}$. L'image de a modulo $(1-a)$ est clairement le neutre $1_{\mathcal{A}}$, mais alors l'image de b par ι est $ab = 0$.

Par exemple, en regardant $a = 3$ et $b = 4$ dans $A = {}^{\mathbb{Z}}\!\big/_{12}$, l'idéal considéré s'écrit $(1-a) = (-2) = (2)$, de sorte que l'algèbre $\mathcal{A}$ se réduit à ${}^{\mathbb{Z}}\!\big/_{2}$ (selon la parité des éléments de A). Un argument de cardinaux suffirait pour conclure à la non injectivité de ι.

Ceci étant dit, soit $P = \sum \lambda_\alpha X^\alpha$ un polynôme de $A[(X_i)]$ et $\overrightarrow{a}$ un I-uplet d'éléments de l'algèbre $\mathcal{A}$.

On peut leur associer un élément de $\mathcal{A}$ en *évaluant* P en $\overrightarrow{a}$, *i.e.* en donnant aux indéterminées la valeur *spéciale* $X_i = a_i$ pour chaque i, l'évaluation étant alors notée $P(\overrightarrow{a})$ ou $P(a)$.

Pour que cette dernière fasse sens (un problème qui n'apparaît qu'avec au moins deux indéterminées), l'évaluation ne doit pas dépendre de la place des indéterminées dans une écriture de P, en particulier de leur ordre dans chaque monôme de P. Comment en effet évaluer le polynôme $XY = YX$ en un couple (a,b), les deux évaluations candidates étant ab et ba ? La commutativité $X_iX_j = X_jX_i$ doit ainsi se répercuter sur la famille $\overrightarrow{a}$ et l'évaluée $P(\overrightarrow{a})$ fera donc sens ssi[2]

$$\forall \alpha \in \operatorname{Supp} P,\ \forall i,j \in \operatorname{Supp}\alpha,\ a_ia_j = a_ja_i.$$

Notons $\mathcal{A}^I_P$ la partie de $\mathcal{A}^I$ formée de tels $\overrightarrow{a}$. On dispose ainsi d'une application ***polynomiale*** (pas d'accent circonflexe sur l'adjectif !)

$$\widetilde{P} := \left\{ \begin{array}{ccc} \mathcal{A}^I_P & \longrightarrow & \mathcal{A} \\ a & \longmapsto & \sum \lambda_\alpha a^\alpha \end{array} \right. .$$

Par ailleurs, raisonnant cette fois à a fixé, évaluer chaque polynôme en a fera sens ssi $\forall P \in A[(X_i)]\,,\ a \in \mathcal{A}^I_P$, *i. e.* ssi[3] les coordonnées de a commutent deux à deux : notons $\mathcal{A}^I_{\text{com}} := \bigcap\limits_{P \in \in A[(X_i)]} \mathcal{A}^I_P$ la partie de $\mathcal{A}^I$ formée de tels a. On dispose alors d'un morphisme d'***évaluation*** (ou de ***spécialisation***)

$$\operatorname{Eval}_a := \left\{ \begin{array}{ccc} A[(X_i)] & \longrightarrow & \mathcal{A} \\ \sum \lambda_\alpha X^\alpha & \longmapsto & \sum \lambda_\alpha a^\alpha \end{array} \right. \text{ si } \forall i,j \in I,\ a_ia_j = a_ja_i.$$

Par exemple, pour $\mathcal{A} = A[(X_i)]$ et $a = \overrightarrow{X} \in \mathcal{A}^I_{\text{com}}$, on trouve

$$\widetilde{P}\left(\overrightarrow{X}\right) = \sum \lambda_\alpha X^\alpha = P.$$

Ceci justifie la notation $P(X)$ pour un polynôme P à une indéterminée : cela dit, cette notation a l'énorme inconvénient que l'on peut rapidement confondre le polynôme formel $P(X)$ avec le scalaire $P(x)$ où x est un point donné, surtout dans les premiers temps.

Proposition.

1. *Si A est intègre infini et ι injectif, alors $P \mapsto \widetilde{P}$ est injectif.*
2. *L'application* Eval_a *fait sens ssi les coordonnées de a commutent deux à deux : dans ce cas,* Eval_a *est un morphisme d'algèbres unitaires ssi chaque coordoonnée de a centralise[4] A.*
3. *Dans le cas d'une seule indéterminée, pour chaques polynômes $P, Q \in A[X]$, si chaque coordoonnée de $\overrightarrow{a}$ commute avec chaque coefficient de Q, on aura alors l'égalité*

$$P(a)\,Q(a) = [PQ](a)\,.$$

Démonstration.

1. L'application $P \mapsto \widetilde{P}$ étant un morphisme de groupes additifs, on invoque un P dans son noyau. En prenant les indéterminées qui apparaissent dans P, on se ramène au cas I fini. Il s'agit donc de montrer que si $P \in A[X_1, ..., X_n]$ vu en tant que fonction polynomiale s'annule sur $\mathcal{A}^n_{\text{com}}$ tout entier, alors P est le polyôme nul. Puisque ι est injectif, on peut imposer P nul sur A^n_{com}. Puisque A est commutatif (car intègre), on peut imposer P nul sur A^n.

[2] On a noté les supports $\operatorname{Supp} P := \left\{\alpha \in \mathbf{N}^{(I)}\ ;\ \lambda_\alpha \neq 0\right\}$ et $\operatorname{Supp}\alpha := \{i \in I\ ;\ \alpha_i \neq 0\}$.

[3] Le sens $\Longleftarrow$ est immédiat, pour le sens $\Longrightarrow$ invoquer $i,j \in I$ et imposer $P := X_iX_j$.

[4] *Rappel* : le ***centre*** d'une partie $P \subset \mathcal{A}$ est formé des éléments de $\mathcal{A}$ qui commutent avec chaque $p \in P$. Un élément ***centralise*** P s'il appartient au centre de P.

Le cas $n = 1$ est immédiat : on plonge A dans son corps des fractions K où P (enfin, son plongé...) admet une infinité de racines (A est infini !), d'où la nullité du plongé et $P = 0$.

Dans le cas général, en considérant l'isomorphisme $A[X_1, ..., X_n] \simeq A[X_1, ..., X_{n-1}][X_n]$, on peut toujours écrire

$$P = \sum_{i_1,...,i_n \geq 0} \lambda_{i_1,...,i_n} X_1^{i_1} ... X_n^{i_n} = \sum_{i \geq 0} \simeq \underbrace{\left(\sum_{i_1,...,i_{n-1} \geq 0} \lambda_{i_1,...,i_{n-1},i} X_1^{i_1} ... X_{n-1}^{i_{n-1}} \right)}_{=: \, P_i(X_1,...,X_{n-1})} X_n^i = \sum_{i \geq 0} P_i (X_1, ..., X_{n-1}) X_n^i$$

Tuons la dernière variable en évaluant en $X_n = a$ pour un a non nul dans A (possible car A est intègre). Par hypothèse, le polynôme à $n - 1$ indéterminées $\sum_{i \geq 0} P_i (X_1, ..., X_{n-1}) a^i$ s'annule sur A^{n-1}, donc est nul par récurrence, ce qui s'écrit

$$\sum_{i \geq 0} \sum_{i_1,...,i_{n-1}} \lambda_{i_1,...,i_{n-1},i} X_1^{i_1} ... X_{n-1}^{i_{n-1}} a^i = 0,$$

ou encore $\lambda_{i_1,...,i_{n-1},i} a^i = 0$ pour chaque $(i_1, ..., i_{n-1}, i)$, d'où $\lambda_{i_1,...,i_n} = 0$ pour chaque $(i_1, ..., i_n)$, *i. e.* $P = 0$.

2. Notons $é$ l'évaluation en a pour alléger les notations. La linéarité de $é$ étant évidente, il s'agit de vérifier $é(PQ) = é(P) é(Q)$ pour deux polynômes $\begin{cases} P = \sum \lambda_\alpha X^\alpha \\ Q = \sum \mu_\alpha X^\alpha \end{cases}$. Cela n'est que du pur calcul formel mais utilise l'hypothèse $\forall i, \forall \lambda \in A, \ a_i \lambda = \lambda a_i$:

$$é(PQ) = \underset{\overrightarrow{a}}{\mathrm{Eval}} \left(\sum_\gamma \left(\sum_{\alpha+\beta=\gamma} \lambda_\alpha \mu_\beta \right) X^\gamma \right) = \sum_\gamma \left(\sum_{\alpha+\beta=\gamma} \lambda_\alpha \mu_\beta \right) a^\gamma \underset{\text{pour chaque } i}{\overset{a_i \text{ centralise } A}{=}} \sum_\alpha \lambda_\alpha a^\alpha \sum_\beta \mu_\beta a^\beta = é(P) é(Q).$$

Réciproquement, supposons l'égalité $é(PQ) = é(P) é(Q)$ pour chaques $P, Q \in A[(X_i)]$, soit $i \in I$ et soit $\lambda \in A$: en imposant $\binom{P}{Q} = \binom{X_i}{\lambda}$, l'hypothèse se réécrit $[X_i \lambda](a) = X_i(a) \lambda(a)$, *i .e.* $[\lambda X_i](a) = a_i \lambda$, ou encore $\lambda a_i = a_i \lambda$, *CQFD*.

Évidemment, on n'oublie pas le caractère unitaire, n'est-ce pas ? De toute façon, il suffit de dire que c'est trivial – parce que ça l'est vraiment !

3. Soient enfin P, Q et a comme dans l'énoncé. En reprenant le calcul établissant l'implication "A commutatif $\Longrightarrow$ $A[(X_i)$ commutatif]", on voit que l'hypothèse sur a permet de valider le même calcul où l'on a remplacé partout X par a, d'où la conclusion[5].

Remarques. Le premier point nous dit qu'il est inutile de distinguer polynômes et fonctions polynomiales (sous les bonnes hypothèses). Le cas le plus courant est celui de $\mathcal{A} = A$ un corps infini, par exemple $A = \mathbb{R}$ ou $\mathbb{C}$. On notera par conséquent toujours $P(\overrightarrow{a})$ au lieu de $\widetilde{P}(\overrightarrow{a})$, quand bien même $P \mapsto \widetilde{P}$ ne serait pas injectif.

Le second point est très utile en algèbre linéaire lorsque l'on parle de polynômes d'endomorphismes. Le cadre est alors $A = k$ un corps et $\mathcal{A} = \mathcal{L}(E)$ où E est un k-ev. Les éléments de A sont alors scalaires, donc centraux et chaque évaluation $K[X] \longrightarrow \mathcal{L}(E)$ est un morphismes d'algèbres.

Noter tout de suite que le neutre $1_\mathcal{A}$ de $\mathcal{L}(E)$ est l'identité Id_E et non la fonction contante égale à 1, qui n'a aucun sens (1 peut-il appartenir à E ?).

La propriété sur le produit permet alors d'écrire des choses agréables comme

$$\prod_{i=1}^n (u - \lambda_i \mathrm{Id}) = \left[\prod_{i=1}^n (X - \lambda_i) \right] (u) = \left(\prod_{i=1}^{n-1} (u - \lambda_i \mathrm{Id}) \right) \circ (u - \lambda_n \mathrm{Id})$$

ou encore

$$P(u) \circ Q(u) = PQ(u) = QP(u) = Q(u) \circ P(u).$$

On renvoie pour une utilisation de ces formules à l'exercice 10 de la première feuille sur les polynômes (qui porte sur le caractère scindé et les opérateurs de dérivations), ainsi qu'au cours sur les invariants de similitudes (réduction de Frobenius).

Quant au dernier point, il raffine le deuxième quand I est un singleton et nous servira pour une démonstration de Cayley-Hamilton où l'on considère l'anneau $A = M_n(K)$ non commutatif.

[5] Dans le cas général, il faut en outre donner sens à $P(a)$ et $Q(a)$ puis justifier les égalités $a^\alpha a^\beta = a^{\alpha+\beta}$ à l'aide d'une hypothèse comme $\begin{matrix} \forall \alpha \in \mathrm{Supp}\, P, \ \forall i \in \mathrm{Supp}\, \alpha, \\ \forall \beta \in \mathrm{Supp}\, Q, \ \forall j \in \mathrm{Supp}\, \beta, \end{matrix}$ $a_i a_j = a_j a_i$, laquelle permet de donner par ailleurs sens à $PQ(a)$ (utiliser l'inclusion $\mathrm{Supp}\, PQ \subset \mathrm{Supp}\, P + \mathrm{Supp}\, Q$).

4 Une application : formalisation des unités en physique

On se donne des unités (J, m, A, kg, W, Hz, K, C, N, Ω, s, mol, V, Pa, cd...) que l'on met dans un ensemble noté $\mathcal{U}$ (comme "**u**nité"), on plonge l'algèbre intègre $\mathbb{R}\left[(X_u)_{u\in\mathcal{U}}\right]$ dans son corps des fractions $\mathbb{R}\left((X_u)_{u\in\mathcal{U}}\right)$ et l'on considère alors l'algèbre intermédiaire

$$\mathbb{R}\left[(X_u)\right] \subset \mathbb{R}\left[X_u, X_u^{-1}\right] \subset \mathbb{R}\left((X_u)\right)$$

engendrée par les indéterminées-unités X_u et leurs inverses X_u^{-1}.

Pourquoi prendre $\mathbb{R}$ comme anneau de base ? Car ses éléments – les nombres réels – ont été précisément conçus pour *mesurer*[6]. Pourquoi dans une algèbre contenant les unités et leurs inverses ? Car l'on pourra, en identifiant abusivement chaque unité $u \in \mathcal{U}$ à son indéterminée correspondante X_u, multiplier et diviser ces unités sans se poser de questions existentielles sur ce qu'est un ohm-newton ou encore un kilogramme-mètre-carré-coulomb-moins-un-seconde-moins-deux (*hint* : c'est un volt).

Comment faire alors apparaître des égalités "dimensionnelles" du type $Hz = \frac{1}{s}$ ou $A = \frac{C}{s}$ ou $J = Ws$ ou encore $N = \frac{kg\ m}{s^2}$? Il suffira de quotienter[7] notre algèbre par les relations analogues au niveau des indéterminées, par exemple (reprenant les égalités précédentes) par l'idéal engendré par $Hz - s^{-1}$, $C - As$, $J - Ws$, et $N - \frac{kg\ m}{s^2}$. On pourra alors écrire des expressions comme

$$3m + \pi\frac{kg}{\Omega^7} - \frac{\sqrt{3}}{s} + c$$

sans avoir l'épée dimensionnelle de Damoclès nous paralysant pour avoir osé additionner une longueur avec une fréquence et une vitesse. Tout ce qui précède montre qu'une telle expresssion est complètement sensée au niveau formel. Lui trouver un sens physique est une tout autre question.

Remarque. Le système MKSA permet d'exprimer n'importe quelle unité à partir de m, kg, s et A. Formellement, cela signifie que l'on peut imposer $\mathcal{U} = \{m, kg, s, A\}$ et retrouver toutes nos unités dans l'algèbre $\mathbb{R}\left[X_u, X_u^{-1}\right]$.

[6] lire par exemple les *Philosophiae naturalis principia mathematica* d'Isaac Newton publiée en 1687

[7] *cf.* mini-cours sur les quotients