

# Polynômes

## Étude algébrique

par **Bernard RANDÉ**

Ancien élève de l'École normale supérieure de Saint-Cloud  
Docteur en mathématiques  
Agrégré de mathématiques  
Professeur de mathématiques spéciales au lycée Saint-Louis

<b>1. Propriétés formelles</b> .....	AF 37 - 2
1.1 Polynômes à plusieurs indéterminées.....	— 2
1.1.1 Présentation de $\mathbb{A}[X_1, \dots, X_n]$ .....	— 2
1.1.2 Polynômes homogènes .....	— 3
1.1.3 Fonctions polynomiales.....	— 3
1.1.4 Dérivations partielles.....	— 4
1.2 Propriétés algébriques .....	— 5
1.2.1 Propriétés lorsque $\mathbb{A}[X]$ est un anneau quelconque.....	— 5
1.2.2 Propriétés élémentaires dans le cas d'un anneau intègre .....	— 5
1.2.3 Le théorème de Hilbert sur les anneaux noethériens.....	— 6
1.3 Propriétés arithmétiques.....	— 6
1.3.1 Algorithme de division euclidienne dans $\mathbb{A}[X]$ .....	— 6
1.3.2 Racines et points d'annulation des polynômes .....	— 7
1.3.3 Arithmétique dans $\mathbb{A}[X]$ .....	— 8
1.4 Polynômes symétriques, antisymétriques de $\mathbb{A}[X_1, \dots, X_n]$ .....	— 12
<b>2. Polynômes irréductibles</b> .....	— 13
2.1 Racines d'un élément de $\mathbb{K}[X]$ .....	— 13
2.1.1 Corps algébriquement clos.....	— 13
2.1.2 Multiplicité des racines .....	— 14
2.1.3 Résolution par radicaux .....	— 15
2.2 Cas des polynômes à coefficients réels.....	— 15
2.2.1 Polynômes irréductibles de $\mathbb{R}[X]$ .....	— 15
2.2.2 Racines de polynômes à coefficients réels.....	— 16
2.3 Factorisation dans $\mathbb{Q}[X]$ .....	— 16
2.3.1 Racines rationnelles d'un élément de $\mathbb{Q}[X]$ .....	— 16
2.3.2 Critères d'irréductibilité dans $\mathbb{Q}[X]$ .....	— 17

**L**es polynômes permettent de résumer les calculs de base sur les nombres : somme, produit, élévation à une puissance entière. C'est la raison pour laquelle ils se sont si tôt introduits comme outils naturels des mathématiques. Formellement, ils sont utilisés comme des schémas universels pour ces calculs, puisque, par substitution, ils permettent de réaliser tout calcul concret à partir de manipulation abstraite.

Dans cet article, nous n'aborderons que les propriétés élémentaires de type algébrique ou arithmétique. Nous nous limiterons aux situations les plus simples, en particulier en ce qui concerne les polynômes irréductibles et la recherche des racines. Les extensions naturelles de l'étude des polynômes sont la géométrie

algébrique réelle, objet de nombreux développements actuels, l'étude des polynômes sur les corps finis, très liés aux codages et, dans une mesure plus abstraite, la géométrie algébrique complexe.

En outre, une étude plus poussée des méthodes numériques de localisation, de séparation et d'approximation des racines réelles ou complexes fera l'objet d'un autre article.

L'article présent suppose connu l'article « Langage des ensembles et des structures » et est à mettre en relation avec les articles relatifs à l'algèbre commutative.

# 1. Propriétés formelles

## 1.1 Polynômes à plusieurs indéterminées

Dans tout ce paragraphe 1.1, on désigne par  $(\mathbb{A}, +, \cdot)$  un anneau commutatif. Le neutre pour l'addition est noté « 0 », le neutre pour la multiplication est noté « 1 ». Le produit de deux éléments  $x$  et  $y$  de  $\mathbb{A}$  sera, le plus souvent, noté  $xy$ .

### 1.1.1 Présentation de $\mathbb{A}[X_1, \dots, X_n]$

Soit  $n$  un entier naturel. Un élément  $\alpha$  de  $\mathbb{N}^n$  est un  $n$ -uplet  $(\alpha_1, \dots, \alpha_n)$ . On utilisera la somme de deux tels  $n$ -uplets :

$$\alpha + \beta = (\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) = (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n).$$

On notera aussi :

$$|\alpha| = \alpha_1 + \dots + \alpha_n.$$

Bien sûr, si  $n = 1$ , on a :  $|\alpha| = \alpha$ .

Soit  $\mathbf{X}$  un symbole. On considère la famille  $(\mathbf{X}^\alpha)_{\alpha \in \mathbb{N}^n}$  de symboles ;  $\mathbf{X}^\alpha$  n'est pas une puissance, mais un nouveau symbole.

Considérons l'ensemble de toutes les expressions :

$$\sum' \lambda_\alpha \mathbf{X}^\alpha,$$

où  $(\lambda_\alpha)$  est une famille presque nulle d'éléments de  $\mathbb{A}$  (que l'on désignera aussi sous le nom de **scalaires**). Cela signifie que tous les  $\lambda_\alpha$  sont nuls, sauf un nombre fini d'entre eux.

Le symbole  $\sum'$  rappelle qu'il s'agit donc d'une somme finie.

On définit, sur l'ensemble de toutes ces expressions, deux lois, par les égalités :

$$\sum' \lambda_\alpha \mathbf{X}^\alpha + \sum' \mu_\alpha \mathbf{X}^\alpha = \sum' (\lambda_\alpha + \mu_\alpha) \mathbf{X}^\alpha ;$$

$$\left(\sum' \lambda_\alpha \mathbf{X}^\alpha\right) \cdot \left(\sum' \mu_\beta \mathbf{X}^\beta\right) = \sum' \left(\sum_{\alpha+\beta=\gamma} \lambda_\alpha \mu_\beta\right) \mathbf{X}^\gamma.$$

Les lois sont donc internes. On définit aussi une loi externe :

$$a \sum' \lambda_\alpha \mathbf{X}^\alpha = \sum' (a \lambda_\alpha) \mathbf{X}^\alpha.$$

Tout particulièrement, notons :

$$X_i = \mathbf{X}^{(0, \dots, 1, \dots, 0)},$$

le 1 étant à la  $j^{\text{ème}}$  place. La définition même du produit conduit aisément à l'égalité :

$$X_i^{\alpha_i} = \mathbf{X}^{(0, \dots, \alpha_i, \dots, 0)},$$

puis :

$$X_1^{\alpha_1} \dots X_n^{\alpha_n} = \mathbf{X}^\alpha \text{ lorsque } \alpha = (\alpha_1, \dots, \alpha_n).$$

On utilisera tantôt l'une, tantôt l'autre notation.

Les symboles  $X_1, \dots, X_n$  sont appelés **indéterminées**. Les expressions ainsi construites sont appelées **polynômes en les  $n$  indéterminées**  $X_1, \dots, X_n$ .

On vérifie que, munie des lois précédentes,  $\mathbb{A}[X_1, \dots, X_n]$  est une  $\mathbb{A}$ -algèbre commutative : l'**algèbre des polynômes en  $n$  indéterminées à coefficients dans  $\mathbb{A}$** .

Lorsque  $n = 0$ , il n'y a pas d'indéterminée. On peut identifier l'algèbre en 0 indéterminée à  $\mathbb{A}$  elle-même.

Par définition, un élément de  $\mathbb{A}[X_1, \dots, X_n]$  peut donc s'écrire, de manière unique, sous la forme :

$$\sum' \lambda_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}.$$

Le scalaire  $\lambda_\alpha$  est appelé **coefficient de  $\mathbf{X}^\alpha$** .

Puisque  $\mathbb{A}[X_1, \dots, X_n]$  est une  $\mathbb{A}$ -algèbre, c'est aussi un  $\mathbb{A}$ -module. Ce qui précède exprime exactement que, en fait,  $\mathbb{A}[X_1, \dots, X_n]$  est un  $\mathbb{A}$ -module **libre**, admettant la **base**  $(\mathbf{X}^\alpha)_{\alpha \in \mathbb{N}^n}$ .

#### ■ Identifications canoniques

Soient  $\sigma$  une permutation de  $[1, n]$  et  $P \in \mathbb{A}[X_1, \dots, X_n]$  ;  $P$  peut aussi s'écrire, de façon unique :

$$P = \sum' \lambda_{\alpha \circ \sigma} X_{\sigma(1)}^{\alpha_{\sigma(1)}} \dots X_{\sigma(n)}^{\alpha_{\sigma(n)}},$$

s'identifiant ainsi à un élément de  $\mathbb{A}[X_{\sigma(1)}, \dots, X_{\sigma(n)}]$ .

Soit, d'autre part,  $m \leq n$ . Tout l'élément  $P$  de  $\mathbb{A}[X_1, \dots, X_n]$  peut également s'écrire :

$$\sum' L_\beta(X_1, \dots, X_m) X_{m+1}^{\beta_{m+1}} \dots X_n^{\beta_n}$$

où  $\beta = (\beta_{m+1}, \dots, \beta_n)$  et où, pour tout  $\beta$ ,  $L_\beta(X_1, \dots, X_m)$  désigne un élément de  $\mathbb{A}[X_1, \dots, X_m]$ . Cette écriture, obtenue par regroupement de termes, est unique. Cela permet d'identifier les  $\mathbb{A}$ -algèbres  $\mathbb{A}[X_1, \dots, X_n]$  et  $\mathbb{A}[X_1, \dots, X_m][X_{m+1}, \dots, X_n]$ .

**Exemple :** pour  $n = 2$ , les quatre  $\mathbb{A}$ -algèbres.

$$\mathbb{A}[X_1, X_2]; \mathbb{A}[X_2, X_1]; \mathbb{A}[X_1][X_2]; \mathbb{A}[X_2][X_1]$$

peuvent être identifiées les unes aux autres. Voici les quatre écritures du même polynôme  $P$  :

$$P = X_1^3 X_2 + 2X_1^2 X_2^2 + X_1 X_2 + X_1^2 \quad (\text{dans } \mathbb{A}[X_1, X_2])$$

$$P = X_2 X_1^3 + 2X_2^2 X_1^2 + X_2 X_1 + X_1^2 \quad (\text{dans } \mathbb{A}[X_2, X_1])$$

$$P = (2X_1^2) X_2^2 + (X_1^3 + X_1) X_2 + X_1^2 \quad (\text{dans } \mathbb{A}[X_1][X_2])$$

$$P = X_2 X_1^3 + (2X_2^2 + 1) X_1^2 + X_2 X_1 \quad (\text{dans } \mathbb{A}[X_2][X_1])$$

■ **Identification de  $\mathbb{A}$  à un sous-anneau de  $\mathbb{A}[X_1, \dots, X_n]$**

L'élément  $\mathbf{X}^0$  (c'est-à-dire  $X_1^0 \dots X_n^0$ ) est le neutre multiplicatif de  $\mathbb{A}[X_1, \dots, X_n]$ . On le note bien sûr « 1 ».

Dans ces conditions, l'application :

$$\begin{aligned} \mathbb{A} &\rightarrow \mathbb{A}[X_1, \dots, X_n] \\ \lambda &\mapsto \lambda \cdot 1 \end{aligned}$$

est un isomorphisme de  $\mathbb{A}$  sur un sous-anneau de  $\mathbb{A}[X_1, \dots, X_n]$ . Cet isomorphisme nous permet d'identifier le scalaire  $\lambda$  avec le polynôme  $\lambda \cdot 1$ , que l'on notera donc  $\lambda$ . L'ensemble des  $\lambda \cdot 1$  est appelé aussi **anneau des polynômes constants**.

■ **Exemples de calculs dans  $\mathbb{A}[X_1, \dots, X_n]$**

Puisque  $\mathbb{A}[X_1, \dots, X_n]$  est un anneau commutatif, on dispose des moyens de calcul les plus habituels :

$$\textcircled{1} \quad \forall k \in \mathbb{N} \quad X_1^k - X_2^k = (X_1 - X_2) \sum_{j=0}^{k-1} X_1^j X_2^{k-1-j}$$

$$\textcircled{2} \quad (X_1 + X_2)^k = \sum_{j=0}^k C_k^j X_1^j X_2^{k-j} \quad (\text{formule du binôme}).$$

$$\textcircled{3} \quad \text{Notons, pour } \alpha \in \mathbb{N}^n, C_k^\alpha \text{ l'entier } \frac{k!}{\alpha_1! \dots \alpha_n!} \text{ lorsque } |\alpha| = k.$$

Alors :

$$(X_1 + \dots + X_n)^k = \sum_{|\alpha|=k} C_k^\alpha \mathbf{X}^\alpha \quad (\text{formule du multinôme}).$$

**1.1.2 Polynômes homogènes**

Les polynômes tels que  $\lambda_\alpha \mathbf{X}^\alpha$ , qui jouent un rôle particulier, sont appelés **monômes**. Le degré du monôme  $\mathbf{X}^\alpha$  est l'entier  $|\alpha|$ . Plus généralement, on a la définition suivante.

**Définition 1.** Soit  $P \in \mathbb{A}[X_1, \dots, X_n]$ . On appelle **degré total** de  $P$ , et on note  $\deg P$ , l'entier naturel :

$$\max \{ |\alpha| \mid \lambda_\alpha \neq 0 \}$$

lorsque  $P$  n'est pas nul et s'écrit :  $P = \sum \lambda_\alpha \mathbf{X}^\alpha$ .

Si  $P = 0$ , on pose :  $\deg P = -\infty$ .

**Exemple :**  $P = X_1^3 X_2^2 - 5X_1^4 + 2X_2^2 X_3^3$  est de degré total égal à 5.

Appelons  $H_d$  l'ensemble des polynômes de  $\mathbb{A}[X_1, \dots, X_n]$  qui sont combinaison linéaire des monômes  $\mathbf{X}^\alpha$ , avec  $|\alpha| = d$ . Un élément de  $H_d$  est appelé **polynôme homogène** de degré (total) égal à  $d$ . Bien sûr,  $H_d$  est stable par combinaison linéaire : c'est donc un  $\mathbb{A}$ -

module ; une base de  $H_d$  est formée des monômes  $\mathbf{X}^\alpha$ , avec  $|\alpha| = d$ . Le nombre de ces monômes est égal à :

$$\text{card} \{ (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n \mid \alpha_1 + \dots + \alpha_n = d \} = \frac{n(n+1)\dots(n+d-1)}{d!}.$$

Il en résulte que  $H_d$  est un  $\mathbb{A}$ -module libre, de dimension égale à :

$$\frac{n(n+1)\dots(n+d-1)}{d!}.$$

Un polynôme  $P$  de  $\mathbb{A}[X_1, \dots, X_n]$  peut s'écrire, de façon unique :

$$P = \sum P_t,$$

où  $P_t$  est homogène de degré  $t$  ; le polynôme  $P_t$  est appelé **partie homogène de degré  $t$**  du polynôme  $P$ . En d'autres termes :

$$\mathbb{A}[X_1, \dots, X_n] = \bigoplus_{t \geq 0} H_t.$$

**Exemple :**  $P = X_1^2 X_2 X_3 + X_2^2 X_3^2 - X_2 + X_3 + 1$

Ainsi :  $P_5 = 0$  ;  $P_4 = X_1^2 X_2 X_3 + X_2^2 X_3^2$  ;  $P_3 = 0$  ;  $P_2 = 0$  ;  
 $P_1 = -X_2 + X_3$  ;  $P_0 = 1$ .

**1.1.3 Fonctions polynomiales**

■ Soit  $\mathbb{B}$  une  $\mathbb{A}$ -algèbre, commutative. Étant donné un polynôme  $P$ , égal à  $\sum \lambda_\alpha \mathbf{X}^\alpha$ , et un  $n$ -uplet  $(x_1, \dots, x_n)$  de  $\mathbb{B}^n$ , on peut considérer l'élément  $\tilde{P}(x_1, \dots, x_n)$  de  $\mathbb{B}$ , défini par l'égalité :

$$\tilde{P}(x_1, \dots, x_n) = \sum \lambda_\alpha x_1^{\alpha_1} \dots x_n^{\alpha_n}.$$

On dit que l'on a donc **substitué**  $x_i$  à  $X_i$  ou, encore, que l'on a **évalué** le polynôme  $P$  en le  $n$ -uplet  $(x_1, \dots, x_n)$ . Le résultat de cette évaluation est parfois tout simplement noté  $P(x_1, \dots, x_n)$ .

**Proposition 1.**

Soient  $\mathbb{B}$  une  $\mathbb{A}$ -algèbre commutative et  $(x_1, \dots, x_n) \in \mathbb{B}^n$ . L'application :

$$\begin{aligned} \mathbb{A}[X_1, \dots, X_n] &\rightarrow \mathbb{B} \\ P &\mapsto \tilde{P}(x_1, \dots, x_n) \end{aligned}$$

est un morphisme d'algèbres.

Cette proposition, qui résulte immédiatement des définitions, permet d'effectuer simplement des calculs sur des expressions polynomiales en un  $n$ -uplet donné : ces calculs s'effectuent tout simplement comme s'il s'agissait de polynômes.

La commutativité de  $\mathbb{B}$ , essentielle, peut être remplacée par la condition plus faible suivante : les  $x_i$  commutent deux à deux.

**Exemples :**

①  $\mathbb{B} = \mathbb{A}$ ,  $n = 1$ .

Soient  $x \in \mathbb{A}$  et  $P \in \mathbb{A}[X_1]$ . Si  $P = \sum_{\alpha=0}^d \lambda_\alpha X_1^\alpha$ , on a :

$$\tilde{P}(x) = \sum_{\alpha=0}^d \lambda_\alpha x^\alpha.$$

②  $\mathbb{B} = \mathbb{A}$ ,  $n$  quelconque.

Soient  $(x_1, \dots, x_n) \in \mathbb{A}^n$  et  $P \in \mathbb{A}[X_1, \dots, X_n]$ . Si  $P = \sum_{|\alpha| \leq d} \lambda_\alpha \mathbf{x}^\alpha$ , on a :

$$\tilde{P}(x_1, \dots, x_n) = \sum_{|\alpha| \leq d} \lambda_\alpha x_1^{\alpha_1} \dots x_n^{\alpha_n}.$$

③  $\mathbb{B} = M_p(\mathbb{A})$ ,  $n = 1$ ,  $(M_p(\mathbb{A}))$  étant l'algèbre des matrices carrées de taille  $p$  à coefficients dans  $\mathbb{A}$ .

Bien sûr,  $\mathbb{B}$  n'est pas commutative en général. On peut néanmoins appliquer ce qui précède pour  $n = 1$  puisque, dans ce cas, la condition de la remarque est satisfaite. Lorsque  $P \in \mathbb{A}[X]$ , l'élément  $P(x)$  est un « polynôme en la matrice  $x$  ».

④  $\mathbb{B} = \mathbb{A}[Y_1, \dots, Y_m]$

Soient  $P$  un élément de  $\mathbb{A}[X_1, \dots, X_n]$  et  $(\chi_1, \dots, \chi_n)$  un  $n$ -uplet de polynômes en les indéterminées  $Y_1, \dots, Y_m$ . On peut alors considérer

$$\tilde{P}(\chi_1, \dots, \chi_n) \in \mathbb{A}[Y_1, \dots, Y_m].$$

Dans le cas particulier où  $n = 1$  et  $m = 1$ , on note aussi  $P \circ \chi$  le polynôme  $\tilde{P}(\chi)$ . Cette notation provient de ce que, si  $x$  est un élément d'une  $\mathbb{A}$ -algèbre, on a :

$$P(\chi)(x) = \tilde{P}(\tilde{\chi})(x).$$

$\tilde{P} \circ \tilde{\chi}$  désignant la composée des applications  $\tilde{P}$  et  $\tilde{\chi}$ . En d'autres termes, on dispose de l'égalité :

$$P \circ \chi = \tilde{P} \circ \tilde{\chi}.$$

■ On considère à présent un entier  $n$  et une  $\mathbb{A}$ -algèbre commutative  $\mathbb{B}$ . L'application :

$$\begin{aligned} \mathbb{A}[X_1, \dots, X_n] &\rightarrow \mathcal{F}(\mathbb{B}^n, \mathbb{B}) \\ P &\mapsto \tilde{P} \end{aligned}$$

est, d'après la proposition 1, un morphisme de la  $\mathbb{A}$ -algèbre  $\mathbb{A}[X_1, \dots, X_n]$  vers la  $\mathbb{A}$ -algèbre  $\mathcal{F}(\mathbb{B}^n, \mathbb{B})$  des applications de  $\mathbb{B}^n$  vers  $\mathbb{B}$ . Son image, l'ensemble des  $\tilde{P}$ , est appelée **algèbre des applications polynomiales** de  $\mathbb{B}^n$  vers  $\mathbb{B}$ .

Plus généralement, si  $D$  est un sous-ensemble de  $\mathbb{B}^n$ , on peut considérer les applications polynomiales sur  $D$ , qui sont les restrictions à  $D$  des applications polynomiales sur  $\mathbb{B}^n$ .

### 1.1.4 Dérivations partielles

Soient  $n$  un entier naturel et  $i \in [1, n]$ . Posons :

$$\forall \alpha \in \mathbb{N}^n \quad D_i (X_1^{\alpha_1} \dots X_n^{\alpha_n}) = \alpha_i X_1^{\alpha_1} \dots X_i^{\alpha_i-1} \dots X_n^{\alpha_n}$$

On peut étendre, de façon unique,  $D_i$  en un endomorphisme linéaire de  $\mathbb{A}[X_1, \dots, X_n]$ , appelé  **$i$ -ième dérivation partielle ou dérivation partielle par rapport à  $X_i$** .

De façon équivalente, si  $P$  s'écrit :

$$P = \sum_{\alpha_i} L_{\alpha_i}(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n) X_i^{\alpha_i},$$

on a :

$$D_i(P) = \sum_{\alpha_i} \alpha_i L_{\alpha_i}(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n) X_i^{\alpha_i-1}.$$

Bien entendu, lorsque  $\alpha_i = 0$ ,  $X_i^{\alpha_i-1}$  n'est pas défini dans  $\mathbb{A}[X_1, \dots, X_n]$ . Cependant,  $\alpha_i X_i^{\alpha_i-1}$  doit être compris comme étant égal à 0.

#### Notations.

- On note aussi  $\frac{\partial P}{\partial X_i}$  le polynôme  $D_i(P)$ .
- Lorsque  $n = 1$  (il y a donc une seule indéterminée), on note  $P'$  plutôt que  $\frac{\partial P}{\partial X_1}$ .

En considérant un élément de  $\mathbb{A}[X_1, \dots, X_n]$  comme un élément de  $\mathbb{A}[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n][X_i]$ , on peut ramener un problème relatif à  $\frac{\partial P}{\partial X_i}$  à un problème relatif à  $P'$ .

#### Proposition 2.

①. Si  $P$  et  $Q$  sont dans  $\mathbb{A}[X_1, \dots, X_n]$ , on a :

$$\forall i \in [1, n] \quad \frac{\partial(PQ)}{\partial X_i} = \frac{\partial P}{\partial X_i} Q + P \frac{\partial Q}{\partial X_i}.$$

②. Si  $P$  est dans  $\mathbb{A}[X_1, \dots, X_n]$ , on a :

$$\forall (i, j) \in [1, n]^2 \quad \frac{\partial}{\partial X_i} \left( \frac{\partial P}{\partial X_j} \right) = \frac{\partial}{\partial X_j} \left( \frac{\partial P}{\partial X_i} \right)$$

#### Preuve. ◊

① Il n'est pas restrictif de supposer  $n = 1$ , et donc d'étudier le cas où  $P$  et  $Q$  sont dans  $\mathbb{A}[X]$ . Si  $P = X^\alpha$  et  $Q = X^\beta$  :

$$(PQ)' = (\alpha + \beta) X^{\alpha + \beta - 1}$$

et  $P'Q + PQ' = \alpha X^{\alpha-1} X^\beta + \beta X^\alpha X^{\beta-1}$ .

L'égalité est vraie dans ce cas. Par bilinéarité, elle est vraie pour  $P$  et  $Q$  quelconques.

② De façon analogue, on peut supposer  $P$  dans  $\mathbb{A}[X_1, X_2]$ . Il suffit alors de vérifier l'égalité pour  $P = X_1^\alpha X_2^\beta$  et de conclure par bilinéarité. ◊

**Notations.** On note le polynôme  $(D_{i_1} \circ \dots \circ D_{i_k})(P)$  :

$$\frac{\partial^k P}{\partial X_{i_1} \dots \partial X_{i_k}}$$

La proposition 2, ②, exprime que  $D_i$  et  $D_j$  commutent. On peut donc donner une forme normalisée à l'expression d'une dérivée partielle en regroupant les dérivations partielles par rapport aux mêmes indéterminées. Ainsi :

$$\frac{\partial^3 P}{\partial X_1 \partial X_2 \partial X_1} = \frac{\partial^3 P}{\partial X_1 \partial X_1 \partial X_2} = \frac{\partial^3 P}{\partial X_1^2 \partial X_2}$$

le symbole «  $\partial X_i^2$  » remplaçant, au dénominateur, le symbole «  $\partial X_1 \partial X_1$  ».

- Si  $n = 1$ , on note  $P^{(k)}$  plutôt que  $\frac{\partial^k P}{\partial X_1^k}$ .

Soit  $P \in \mathbb{A}[X_1, \dots, X_n]$ , considéré comme un élément de  $\mathbb{A}[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n][X_i]$  :

$$P = \sum_{\alpha_i} L_{\alpha_i}(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n) X_i^{\alpha_i}.$$

Le **degré partiel de  $P$  par rapport à  $X_i$**  est, par définition, le plus grand des entiers  $\alpha_i$  tels que  $L_{\alpha_i}$  soit non nul. Le degré partiel du polynôme nul par rapport à  $X_i$  est  $-\infty$ ; on note  $\deg_{X_i} P$  le degré partiel de  $P$  par rapport à  $X_i$ .

**Exemple :** soit  $P = X_1^3 X_2^2 + X_2^4 + 1$ .

On a :  $\deg_{X_1} P = 3$  ;  $\deg_{X_2} P = 4$ .

Remarquons que le degré total de  $P$  est égal à 5.

**Cas particulier.**

Lorsqu'il n'y a qu'une seule indéterminée, le degré partiel par rapport à cette indéterminée et le degré total sont égaux. On l'appellera **degré** du polynôme considéré. D'autre part, si  $P$  est de degré  $d \geq 0$ , on peut écrire :

$$P = \sum_{k=0}^d a_k X^k,$$

avec  $a_d \neq 0$ .

Ce scalaire  $a_d$  est appelé **coefficient dominant** du polynôme  $P$ . Lorsque  $a_d = 1$ , on dit aussi que  $P$  est **unitaire** (ou encore **normalisé**).

Remarquons, dans ce cas, l'inégalité évidente :

$$\deg(P + Q) \leq \max(\deg P, \deg Q).$$

## 1.2 Propriétés algébriques

### 1.2.1 Propriétés lorsque $\mathbb{A}$ est un anneau quelconque

Dans ce paragraphe 1.2.1,  $\mathbb{A}$  est un anneau commutatif.

**Proposition 3.**

Soit  $P \in \mathbb{A}[X]$ . On pose  $d = \deg P$  et  $P = \sum_{k=0}^d a_k X^k$ .

①  $P$  est inversible dans  $\mathbb{A}[X]$  si, et seulement si,  $a_0$  est inversible dans  $\mathbb{A}$  et  $a_1, \dots, a_d$  sont nilpotents.

②  $P$  est nilpotent si, et seulement si,  $a_0, a_1, \dots, a_d$  sont nilpotents.

③  $P$  est un diviseur de 0 dans  $\mathbb{A}[X]$  si, et seulement si, il existe  $\lambda \in \mathbb{A} \setminus \{0\}$  tel que  $\lambda P = 0$ .

**Preuve.** ♦

① Supposons  $P$  inversible, d'inverse  $Q = \sum_{k=0}^e b_k X^k$ , où  $e$  désigne le degré de  $Q$ .

Ainsi :  $\sum_{k=0}^{d+e} \left( \sum_{i+j=k} a_i b_j \right) X^k = 1$ .

Plaçons-nous dans le cas où  $d \geq 1$ .

En particulier :  $a_d b_e = 0$ .

Montrons par récurrence sur  $m$  que  $a_d^{m+1} b_{e-m} = 0$ .

Cette propriété est vraie pour  $m = 0$ .

Supposons-la vraie pour tous les indices  $\leq m$ , avec  $m \leq e - 1$ . On a :

$$\sum_{i+j=d+e-m-1} a_i b_j = 0$$

car  $d + e - m - 1 \geq 1$ . Donc :

$$a_d b_{e-m-1} + a_{d-1} b_{e-m} + \dots = 0$$

Multiplions cette égalité par  $a_d^{m+1}$ . On a, grâce à l'hypothèse de récurrence :

$$a_d^{m+1} b_{e-m} = 0 ; a_d^{m+1} b_{e-m+1} = a_d \cdot a_d^m b_{e-m+1} = 0 ; \text{etc.}$$

Donc :  $a_d^{m+2} b_{e-m-1} = 0$ .

Appliquée à  $m = e$ , cette propriété montre que  $a_d$  est nilpotent.

Donc  $P - a_d X^d$ , différence entre un inversible et un nilpotent, est inversible. Il résulte d'une hypothèse de récurrence non formulée sur  $\deg P$  que  $a_0$  est inversible ;  $a_1, \dots, a_{d-1}$  sont nilpotents.

Il faut vérifier que le résultat est vrai pour  $d = 0$ . Dans ce cas, on obtient  $a_0 b_0 = 1$ . Donc  $a_0$  est bien inversible.

Si, réciproquement,  $a_0$  est inversible et  $a_1, \dots, a_d$  sont nilpotents, alors  $a_1 X + \dots + a_d X^d$  est encore nilpotent, comme somme de nilpotents. Donc  $P$ , somme d'un inversible et d'un nilpotent, est inversible.

② Si  $P$  est nilpotent, il existe  $k$  tel que  $P^k = 0$ . En particulier,  $a_d^k = 0$ , donc  $a_d$  est nilpotent. Par conséquent,  $P - a_d X^d$  est nilpotent et, grâce à une hypothèse de récurrence sur  $\deg P$ ,  $a_0, a_1, \dots, a_{d-1}$  sont nilpotents.

Si  $a_0, \dots, a_d$  sont nilpotents,  $P$  est nilpotent comme somme de nilpotents.

③ Parmi tous les polynômes non nuls  $Q$  tels que  $PQ = 0$ , choisissons-en un de degré  $e$  minimal. On a, par considération du coefficient de  $X^{d+e}$ ,  $a_d b_e = 0$  (si  $Q = \sum_{k=0}^e b_k X^k$ ). Par conséquent,

puisque  $(a_d Q) P = 0$  et que  $\deg(a_d Q) \leq e - 1$ , on a :  $a_d Q = 0$ .

Montrons par récurrence que  $a_{d-m} Q = 0$ .

Supposons cette propriété vraie pour tous les indices  $\leq m$ , où  $m \leq d - 1$ . On dispose de l'égalité :

$$\sum_{i+j=d+e-m-1} a_i b_j = 0$$

Donc :  $a_{d-m-1} b_e + a_{d-m} b_{e-1} + \dots = 0$ .

Mais  $a_{d-m} Q = 0$ , donc  $a_{d-m} b_{e-1} = 0$ , et de même pour les termes suivants.

On a donc  $a_{d-m-1} b_e = 0$  et le même raisonnement que précédemment prouve que :  $a_{d-m-1} Q = 0$ .

Ainsi, on a :  $\forall k \ a_k Q = 0$  et, en particulier, puisque  $Q$  est non nul et qu'il existe  $i$  tel que  $b_i \neq 0$  :

$$\forall k \ a_k b_i = 0$$

Par conséquent  $b_i P = 0$ , ce que l'on voulait prouver.

La réciproque est évidente. ♦

### 1.2.2 Propriétés élémentaires dans le cas d'un anneau intègre

Dans ce paragraphe 1.2.2, on suppose que  $\mathbb{A}$  est un anneau commutatif **intègre**.

**Proposition 4.**

Si  $P$  et  $Q$  sont dans  $\mathbb{A}[X]$ , on a :

$$\deg PQ = \deg P + \deg Q.$$

De plus,  $\mathbb{A}[X]$  est intègre.

**Preuve.** ♦ Supposons d'abord  $P$  et  $Q$  non nuls, de degrés  $d$  et  $e$ .

Alors, en posant :

$$P = \sum_{k=0}^d a_k X^k, \quad Q = \sum_{k=0}^e b_k X^k,$$

on a :

$$PQ = \sum_{k=0}^{d+e} \left( \sum_{i+j=k} a_i b_j \right) X^k.$$

Le coefficient de  $X^{d+e}$  dans  $PQ$  est  $a_d b_e$ , non nul comme produit d'éléments non nuls. Donc :

$$\deg PQ = d + e .$$

■ Si  $P$  ou  $Q$  est nul, chacun des deux membres est égal à  $-\infty$ .

En particulier, si  $P$  et  $Q$  sont non nuls,  $PQ$  est non nul. Donc  $\mathbb{A}[X]$  est intègre. ◊

**Corollaire 1.**  $\mathbb{A}[X_1, \dots, X_n]$  est intègre.

**Preuve.** ◊ Cela résulte de l'identification de  $\mathbb{A}[X_1, \dots, X_n]$  à  $\mathbb{A}[X_1, \dots, X_{n-1}][X_n]$  et du fait que, par récurrence,  $\mathbb{A}[X_1, \dots, X_{n-1}]$  est intègre. ◊

**Corollaire 2.** Si  $P$  et  $Q$  sont dans  $\mathbb{A}[X_1, \dots, X_n]$ , alors :

$$\forall i \in [1, n] \quad \deg_{X_i} PQ = \deg_{X_i} P + \deg_{X_i} Q .$$

**Proposition 5.**

Si  $P$  et  $Q$  sont dans  $\mathbb{A}[X_1, \dots, X_n]$ , alors :

$$\deg PQ = \deg P + \deg Q .$$

**Preuve.** ◊ Écrivons  $P = \sum_{t=0}^d P_t$  et  $Q = \sum_{t=0}^e Q_t$ , où  $d, e$  sont les degrés totaux de  $P, Q$  et où  $P_t, Q_t$  sont des polynômes homogènes de degré  $t$ . Alors :

$$PQ = \sum_{t=0}^{d+e} \left( \sum_{i+j=t} P_i Q_j \right) .$$

Puisque  $\mathbb{A}[X_1, \dots, X_n]$  est intègre,  $P_d Q_e \neq 0$ . Donc :  $\deg PQ = d + e$ . ◊

**Proposition 6.**

Soit  $P \in \mathbb{A}[X_1, \dots, X_n]$ . Il y a équivalence entre :

- ①  $P$  est inversible dans  $\mathbb{A}[X_1, \dots, X_n]$  ;
- ②  $P$  est un élément de  $\mathbb{A}$ , inversible dans  $\mathbb{A}$ .

**Preuve.** ◊ Bien que ce résultat soit une conséquence de la proposition 3, le cadre usuel dans lequel nous nous plaçons mérite une démonstration directe.

②  $\Rightarrow$  ① est clair.

①  $\Rightarrow$  ② Soit  $Q$  l'inverse de  $P$ . On a :

$$\deg (PQ) = 0$$

car 1 est de degré 0. Donc  $\deg P = \deg Q = 0$ .

En particulier,  $P \in \mathbb{A}$  ; comme  $Q \in \mathbb{A}$ ,  $P$  est bien inversible dans  $\mathbb{A}$ . ◊

### 1.2.3 Le théorème de Hilbert sur les anneaux noethériens

Rappelons qu'un anneau  $\mathbb{A}$  est dit **noethérien** lorsque toute suite croissante d'idéaux de  $\mathbb{A}$  est stationnaire. Un cas particulier d'anneau noethérien est celui d'un anneau **principal**. La plupart des anneaux usuels en algèbre élémentaire sont noethériens. Le théorème suivant montre que les anneaux de polynômes sur un anneau noethérien sont encore noethériens.

**Théorème 1 (Hilbert).** Si  $\mathbb{A}$  est un anneau noethérien,  $\mathbb{A}[X_1, \dots, X_n]$  est un anneau noethérien.

**Preuve.** ◊ Grâce à l'identification de  $\mathbb{A}[X_1, \dots, X_n]$  avec  $\mathbb{A}[X_1, \dots, X_{n-1}][X_n]$  et un raisonnement par récurrence, on peut supposer  $n = 1$ . On appelle  $X$  l'unique indéterminée.

Soit  $I$  un idéal quelconque de  $\mathbb{A}[X]$ . On note  $d_n(I)$  l'ensemble des coefficients dominants des éléments de  $I$  qui sont exactement

de degré  $n$ , auxquels on ajoute 0. Il est facile de voir que  $d_n(I)$  est un idéal de  $\mathbb{A}$ . D'autre part, la suite  $(d_k(I))_{k \geq 0}$  est croissante, car, si  $P$  appartient à  $I$ ,  $XP$  appartient aussi à  $I$ .

■ Considérons, à présent, une suite croissante  $(I_n)_{n \geq 0}$  d'idéaux de  $\mathbb{A}[X]$ . La suite  $(d_n(I_n))_{n \geq 0}$  est alors croissante. En effet, on a :

$$d_n(I_n) \subset d_n(I_{n+1}) \text{ car } I_n \subset I_{n+1}, \text{ et } d_n(I_{n+1}) \subset d_{n+1}(I_{n+1}) .$$

La suite  $(d_n(I_n))_{n \geq 0}$  est donc stationnaire, égale à  $d_p(I_p)$ .

Il est clair que  $d_p(I_p)$  contient tous les  $d_k(I_n)$ , puisque, en posant  $r = \max(k, n, p)$ , on a :

$$d_k(I_n) \subset d_r(I_n) \subset d_r(I_r) = d_p(I_p) .$$

■ Considérons, par ailleurs, les suites  $(d_0(I_n))_{n \geq 0}, \dots, (d_{p-1}(I_n))_{n \geq 0}$ . Elles sont toutes stationnaires, à partir d'un indice  $q$  que l'on peut supposer supérieur ou égal à  $p$ .

Soit alors  $n \geq q$ . Montrons que, pour tout  $k$  :

$$d_k(I_q) = d_k(I_n) .$$

**Premier cas :**  $k \geq p$ .

On a :

$$d_k(I_q) \subset d_k(I_n) \subset d_p(I_p) \subset d_k(I_p) \subset d_k(I_q) ,$$

d'où l'égalité.

**Deuxième cas :**  $k \leq p - 1$ .

On a alors :

$$d_k(I_n) = d_k(I_q)$$

grâce à la constance de  $(d_k(I_n))_{n \geq q}$ .

■ Montrons, finalement, que  $I_n = I_q$ . On a  $I_q \subset I_n$ . Montrons par récurrence sur  $e = \deg P$  que, si  $P \in I_n$ , alors :  $P \in I_q$ .

Le résultat est supposé vrai pour les polynômes de degré  $\leq e - 1$ . Soit  $P$  de degré  $e$ , appartenant à  $I_n$ . Puisque  $d_e(I_n) = d_e(I_q)$ , il existe  $Q \in I_q$  tel que  $Q = a_e X^e + \dots$  lorsque  $a_e$  est le coefficient dominant de  $P$ . Dans ces conditions :

$$\deg (P - Q) \leq e - 1$$

et  $P - Q \in I_n$ . Donc :

$$P - Q \in I_q \text{ et } P \in I_q .$$

Ainsi, la suite  $(I_n)$  est stationnaire à partir du rang  $q$ . ◊

## 1.3 Propriétés arithmétiques

### 1.3.1 Algorithme de division euclidienne dans $\mathbb{A}[X]$

**Théorème 2.** Soient  $\mathbb{A}$  un anneau commutatif et  $N$  et  $D$  deux éléments de  $\mathbb{A}[X]$ . On suppose que  $D$  est non nul, et que son coefficient dominant est inversible dans  $\mathbb{A}$ .

Il existe alors un unique couple  $(Q, R) \in \mathbb{A}[X]^2$  tel que :

$$N = DQ + R$$

et

$$\deg R \leq (\deg D) - 1 .$$

**Preuve.** ♦

① **Unicité**

Si  $(Q, R)$  et  $(Q_1, R_1)$  sont solutions du problème, on a :

$$D(Q - Q_1) = R_1 - R$$

Or  $\deg(R_1 - R) \leq (\deg D) - 1$  et, si  $Q \neq Q_1$ , on a :

$$\deg D(Q - Q_1) = \deg D + \deg(Q - Q_1)$$

car le coefficient dominant de  $D$  est inversible. Donc :

$$\deg D(Q - Q_1) \geq \deg D$$

Il y a contradiction.

Il est donc nécessaire que  $Q = Q_1$ , puis que  $R = R_1$ .

② **Existence.**

Lorsque  $\deg N \leq (\deg D) - 1$ , il suffit de prendre  $Q = 0, R = N$ .

Raisonnons ensuite par récurrence sur  $\deg N$ . On pose :

$$N = a_k X^k + \dots$$

$$D = b_\ell X^\ell + \dots \text{ avec } b_\ell \text{ inversible dans } \mathbb{A}.$$

On construit deux suites  $(Q_i)_{i \in [\ell-1, k]}$  et  $(R_i)_{i \in [\ell-1, k]}$  de polynômes tels que :

$$N = DQ_i + R_i, \text{ avec } \deg R_i \leq i.$$

C'est possible pour  $i = k$ , en prenant  $Q_k = 0, R_k = N$ .

Supposons construits  $Q_i$  et  $R_i$ . Posant  $R_i = \lambda X^i + \dots$ , on définit :

$$R_{i-1} = R_i - \lambda b_\ell^{-1} DX^{i-\ell}.$$

Alors :

$$\begin{aligned} N &= DQ_i + \lambda b_\ell^{-1} DX^{i-\ell} + R_{i-1} \\ &= DQ_{i-1} + R_{i-1} \text{ avec } \deg R_{i-1} \leq i-1. \end{aligned}$$

Dans ces conditions,  $R_{\ell-1}$  est le reste cherché et  $Q_{\ell-1}$ , le quotient. En fait,  $\lambda b_\ell^{-1} X^{i-\ell}$  est le monôme de degré  $i-\ell$  de  $Q$ , qui se construit ainsi petit à petit en partant des termes de plus haut degré.

Cet algorithme, appelé **stathme** de la division euclidienne, correspond à la division à la main.

**Exemple :**  $N = 2X^4 + X^3 - X + 2 ; D = X^2 + 2X + 1$

L'anneau  $\mathbb{A}$  est ici égal à  $\mathbb{Z}$ .

$R_4 = N$	$2X^4 + X^3 - X + 2$	$X^2 + 2X + 1$	$D$
$R_3$	$-3X^3 - 2X^2 - X + 2$	$2X^2$	$Q_3$
$R_2$	$4X^2 + 2X + 2$	$2X^2 - 3X$	$Q_2$
$R_1 = R$	$-6X - 2$	$2X^2 - 3X + 4$	$Q_1 = Q$

### 1.3.2 Racines et points d'annulation des polynômes

**Définition 2.** Soit  $P \in \mathbb{A}[X]$ . On dit que l'élément  $\alpha$  de  $\mathbb{A}$  est racine de  $P$  lorsque  $\tilde{P}(\alpha) = 0$ .

**Proposition 7.**

Si  $\mathbb{A}$  est un anneau commutatif, il y a équivalence entre :

- i)  $\alpha$  est racine de  $P$  ;
- ii)  $X - \alpha$  divise  $P$ .

**Preuve.** ♦ Dire que  $X - \alpha$  divise  $P$ , c'est affirmer l'existence d'un polynôme  $Q$  tel que  $P = (X - \alpha)Q$ .

ii)  $\Rightarrow$  i) est immédiat.

i)  $\Rightarrow$  ii) Effectuons la division euclidienne de  $P$  par  $X - \alpha$  (c'est possible car 1 est inversible). On peut écrire :

$$P = (X - \alpha)Q + R$$

où  $\deg R \leq 0$ , ce qui signifie que  $R \in \mathbb{A}$ . Évaluant en  $\alpha$ , on obtient  $R = 0$ .

Dans la suite de ce paragraphe, et jusqu'à la fin de l'article, on suppose que  $\mathbb{A}$  est un anneau intègre.

**Proposition 8.**

Soit  $\mathbb{A}$  un anneau intègre. Si  $P \in \mathbb{A}[X] - \{0\}$  et si  $\deg P \leq d$ ,  $P$  admet au plus  $d$  racines.

**Preuve.** ♦ Soit  $\alpha_1$  une racine de  $P$ . On peut écrire :

$$P = (X - \alpha_1)Q \text{ avec } \deg Q \leq d - 1.$$

Une racine  $\alpha$  de  $P$ , différente de  $\alpha_1$ , est nécessairement une racine de  $Q$  car  $(\alpha - \alpha_1)Q(\alpha) = 0$  et  $\alpha - \alpha_1 \neq 0$ . Comme, par récurrence,  $Q$  (qui est non nul) admet au plus  $d - 1$  racines,  $P$  admet bien au plus  $d$  racines.

Ainsi, pour montrer que deux polynômes  $P$  et  $Q$  sont égaux, il suffit de montrer qu'ils prennent les mêmes valeurs en  $(d + 1)$  points distincts, où  $d \geq \deg(P - Q)$ . En effet, dans ce cas,  $P - Q$  ne pourra appartenir à  $\mathbb{A}[X] - \{0\}$ , donc sera nul.

**Corollaire 1.** Soit  $D$  un sous-ensemble infini de l'anneau intègre  $\mathbb{A}$ . L'application  $P \mapsto \tilde{P}$  qui, au polynôme  $P$  de  $\mathbb{A}[X]$ , associe l'application polynomiale correspondante sur  $D$ , est injective.

Ce corollaire 1, qui se prouve en remarquant que, si  $\tilde{P} = 0$ ,  $P$  admet une infinité de racines, donc est nul, admet une extension convenable dans le cas des polynômes à  $n$  indéterminées.

**Corollaire 2.** Soit  $D = D_1 \times \dots \times D_n$  un produit d'ensembles infinis. L'application  $P \mapsto \tilde{P}$  qui, au polynôme  $P$  de  $\mathbb{A}[X_1, \dots, X_n]$ , associe l'application polynomiale correspondante sur  $D$ , est injective.

**Preuve.** ♦ Pour  $n = 1$ , il s'agit du corollaire 1. On suppose le résultat vrai à l'ordre  $n - 1$ . Soit  $P \in \mathbb{A}[X_1, \dots, X_n]$  tel que :

$$\forall (x_1, \dots, x_n) \in D \quad \tilde{P}(x_1, \dots, x_n) = 0.$$

On peut écrire :

$$P = \sum_i L_i(X_1, \dots, X_{n-1}) X_n^i,$$

et considérer ainsi  $P$  comme un élément de  $\mathbb{B}[X_n]$ , avec  $\mathbb{B} = \mathbb{A}[X_1, \dots, X_{n-1}]$ . Fixons  $(x_1, \dots, x_{n-1}) \in D_1 \times \dots \times D_{n-1}$ .

On a donc :

$$\forall x_n \in D_n \quad \sum_i L_i(x_1, \dots, x_{n-1}) x_n^i = 0.$$

Cela exprime que le polynôme  $\sum_i L_i(x_1, \dots, x_{n-1}) X_n^i$  admet une infinité de racines, à savoir tous les éléments de  $D_n$  ; il est donc nul. Par conséquent :

$$\forall i \quad L_i(x_1, \dots, x_{n-1}) = 0.$$

Cela étant réalisé pour tout  $(x_1, \dots, x_{n-1})$  dans  $D_1 \times \dots \times D_{n-1}$ , l'hypothèse de récurrence entraîne que tous les  $L_i$  sont nuls. Donc  $P = 0$ .

Il ne faudrait pas croire qu'un polynôme  $P \in \mathbb{A}[X_1, \dots, X_n]$  tel que  $\tilde{P}$  s'annule sur un ensemble infini quelconque est nécessairement nul. Par exemple, si  $n = 2$ , l'ensemble des  $(x_1, x_2)$  de  $\mathbb{R}^2$  tels que  $x_1 = 0$  est infini (c'est une droite !). Pourtant  $X_1$  n'est pas le polynôme nul.

### 1.3.3 Arithmétique dans $\mathbb{A}[X]$

#### 1.3.3.1 Rappels de vocabulaire

Dans ce paragraphe, nous rappelons le langage de la **divisibilité** dans un anneau commutatif intègre  $\mathbb{B}$ .

■ On appelle **idéal (principal)** engendré par l'élément  $a$  de  $\mathbb{B}$  l'ensemble, noté  $a\mathbb{B}$ , des multiples de  $a$ :

$$a\mathbb{B} = \{ab\}_{b \in \mathbb{B}}.$$

On dit que  $a$  **divise**  $c$ , et on note  $a|c$ , lorsqu'il existe  $b$  dans  $\mathbb{B}$  tel que  $c = ab$ . Autrement dit :

$$a|c \Leftrightarrow c \in a\mathbb{B} \Leftrightarrow c\mathbb{B} \subset a\mathbb{B}.$$

On dit que les éléments  $a$  et  $c$  sont **associés** lorsqu'ils se divisent mutuellement. On a :

$$a \text{ et } c \text{ sont associés} \Leftrightarrow c\mathbb{B} = a\mathbb{B}.$$

Notons  $U(\mathbb{B})$  l'ensemble des éléments inversibles de  $\mathbb{B}$ ; il s'agit d'un **groupe multiplicatif**. On dispose de l'équivalence :

$$c\mathbb{B} = a\mathbb{B} \Leftrightarrow \exists \lambda \in U(\mathbb{B}) \quad a = \lambda b \Leftrightarrow \exists \mu \in U(\mathbb{B}) \quad b = \mu a.$$

■ Soit  $p$  un élément de  $\mathbb{B}$ . On dit que  $p$  est **irréductible** lorsque  $p \notin U(\mathbb{B})$  et que :

$$p = ab \Rightarrow p \text{ associé à } a \text{ ou } p \text{ associé à } b.$$

Cette dernière condition équivaut à dire que  $p$  n'est divisible que par les inversibles et les éléments qui lui sont associés.

■ Soient  $a$  et  $b$  deux éléments de  $\mathbb{B}$ . On dit qu'ils sont **premiers entre eux** lorsque :

$$d|a \text{ et } d|b \Rightarrow d \in U(\mathbb{B}).$$

En d'autres termes, ils admettent les inversibles pour seuls diviseurs communs.

■ Soit  $(a_i)_{i \in I}$  une famille d'éléments de  $\mathbb{B}$ . L'idéal engendré par cette famille est, par définition, le plus petit idéal de  $\mathbb{B}$  contenant  $\{a_i\}_{i \in I}$ . On le note  $\sum_{i \in I} a_i \mathbb{B}$ . Il est égal à :

$$\left\{ \sum_{i \in I} a_i b_i \right\}_{(b_i) \in \mathbb{B}^{(I)}}.$$

Comme d'habitude, il s'agit de sommes finies.

#### 1.3.3.2 Étude de $\mathbb{K}[X]$ ( $\mathbb{K}$ corps)

Dans tout ce paragraphe,  $\mathbb{K}$  est un **corps**.

Puisque tout élément non nul de  $\mathbb{K}$  est inversible, le théorème 2 s'applique dès que  $D$  n'est pas le polynôme nul. Cela a une conséquence importante.

**Théorème 3.**  $\mathbb{K}[X]$  est un anneau principal.

**Preuve.** ◊ Il s'agit de prouver que tout idéal  $I$  de  $\mathbb{K}[X]$  est principal, c'est-à-dire qu'il est de la forme  $D \cdot \mathbb{K}[X] = \{DQ\}_{Q \in \mathbb{K}[X]}$ , pour un certain polynôme  $D$ .

On peut évidemment supposer  $I \neq \{0\}$ .

Soit  $D$  un polynôme de  $I - \{0\}$  qui est de plus petit degré. On a, bien sûr, l'inclusion  $D \cdot \mathbb{K}[X] \subset I$ , puisque  $D \in I$ .

Soit, réciproquement,  $N$  un élément de  $I$ . Puisque  $D \neq 0$ , il existe  $(Q, R) \in \mathbb{K}[X]^2$  tel que :

$$N = DQ + R \quad \text{avec} \quad \deg R \leq (\deg D) - 1.$$

Or :  $R = N - DQ \in I$ , puisque  $N \in I$  et  $DQ \in I$ .

Comme  $\deg R < \deg D$ , on a :

$$R = 0, \text{ puis } N = DQ. \quad \diamond$$

Ce théorème permet d'appliquer à  $\mathbb{K}[X]$  l'**arithmétique usuelle**, c'est-à-dire celle à laquelle on est accoutumé dans l'anneau des entiers relatifs.

Soit  $I$  un idéal de  $\mathbb{K}[X]$ . Le théorème 3 assure qu'il existe un polynôme  $\Delta$  tel que  $I = \Delta \mathbb{K}[X]$ . Un tel polynôme  $\Delta$  est appelé un **générateur** de  $I$ . Il n'est pas unique : les générateurs de  $I$  sont les éléments associés à  $\Delta$ .

Si  $I \neq \{0\}$ ,  $\Delta$  n'est pas le polynôme nul. Soit  $\lambda$  son coefficient dominant ;  $\frac{1}{\lambda} \Delta$  est alors unitaire et, précisément, c'est l'unique polynôme unitaire qui engendre  $I$ . On parlera, par abus de langage, du **générateur** de  $I$ , le contexte devant rendre clair ce choix.

Bien entendu, si  $I = \{0\}$ , son seul générateur est le polynôme nul. Remarquons, d'autre part, qu'un générateur de  $I$  est caractérisé par le fait que c'est l'élément non nul de  $I$  de plus petit degré.

■ Soit  $(Q_i)_{i \in I}$  une famille d'éléments de  $\mathbb{K}[X]$ . L'idéal  $\sum_{i \in I} Q_i \mathbb{K}[X]$ , formé des sommes  $\sum_{i \in I} Q_i U_i$ , où  $(U_i)$  décrit l'ensemble des familles presque nulles de polynômes, est un idéal principal. Soit  $\Delta$  un générateur de cet idéal. On dit que  $\Delta$  est un **plus grand commun diviseur** de la famille  $(Q_i)_{i \in I}$ , en abrégé :

$$\Delta = \text{pgcd} (Q_i)_{i \in I}.$$

Le plus souvent, on prend un générateur particulier : l'unique générateur unitaire lorsque  $\sum_{i \in I} Q_i \mathbb{K}[X] \neq \{0\}$ , et 0 sinon. Tous les pgcd sont associés à celui-ci.

#### ■ Caractérisation d'un pgcd

Pour que  $\Delta$  soit un pgcd de la famille  $(Q_i)_{i \in I}$ , il faut et il suffit qu'il vérifie la double condition :

$$\forall i \in I \quad \Delta | Q_i;$$

si

$$\forall i \in I \quad D | Q_i, \text{ alors } D | \Delta.$$

Autrement dit, pour la relation de divisibilité,  $\Delta$  est un « plus grand élément » de l'ensemble des diviseurs communs aux  $Q_i$ ; cette dénomination est quelque peu abusive, dans la mesure où la relation de divisibilité dans  $\mathbb{K}[X]$  est une **relation de préordre**, et pas une relation d'ordre.

On peut remarquer aussi qu'un pgcd de la famille  $(Q_i)_{i \in I}$  est un polynôme de plus grand degré qui divise tous les  $Q_i$ , ce qui justifie autrement cette dénomination.

#### ■ Relation de Bezout

Soit  $\Delta = \text{pgcd} (Q_i)_{i \in I}$ . Il existe alors une famille presque nulle  $(U_i)_{i \in I}$  de polynômes telle que :

$$\Delta = \sum_{i \in I} Q_i U_i.$$

Cette relation exprime que  $\Delta \in \sum_{i \in I} Q_i \mathbb{K}[X]$ .

On dit que la famille des  $(Q_i)_{i \in I}$  est formée d'éléments premiers entre eux dans leur ensemble lorsque :  $1 = \text{pgcd}(Q_i)_{i \in I}$ . On a l'équivalence suivante :

$$1 = \text{pgcd}(Q_i)_{i \in I} \Leftrightarrow \exists (U_i)_{i \in I} \quad 1 = \sum_{i \in I} Q_i U_i .$$

L'implication de gauche à droite n'est rien d'autre que la propriété générale d'un pgcd dans un anneau principal ci-dessus.

L'implication de droite à gauche résulte du fait que, si  $1 \in \sum_{i \in I} Q_i \mathbb{K}[X]$ , alors  $\sum_{i \in I} Q_i \mathbb{K}[X] = \mathbb{K}[X]$ .

Les propriétés du pgcd dans  $\mathbb{K}[X]$  sont celles vérifiées dans tout anneau principal. Nous ne les rappellerons pas en détail. Un point important est que le **stathme** de division euclidienne permet des calculs effectifs de pgcd, ainsi que des **coefficients de Bezout**, c'est-à-dire des polynômes  $U_i$ . Pratiquement, on se limite à deux polynômes, puis on utilise la propriété d'associativité suivante :

$$\text{pgcd}(Q_1, \dots, Q_n) = \text{pgcd}(\text{pgcd}(Q_1, \dots, Q_{n-1}), Q_n) .$$

**■ Algorithme d'Euclide**

L'algorithme d'Euclide permet de déterminer le pgcd de deux polynômes et, en outre, de déterminer deux polynômes coefficients d'une relation de Bezout.

**Notation**

Soit  $D$  un polynôme non nul. On désigne par  $N \text{ mod } D$  le reste de la division de  $N$  par  $D$ ; on lit ceci «  $N$  modulo  $D$  ».

On remarque que, si  $D \neq 0$  :

$$\text{pgcd}(N, D) = \text{pgcd}(D, N \text{ mod } D) .$$

En effet, un diviseur de  $N$  et  $D$  divise aussi  $N \text{ mod } D$ , qui est de la forme  $N - QD$ . De même, un diviseur de  $D$  et de  $N \text{ mod } D$  divise  $N$ . Cela fournit l'algorithme suivant ; on pose  $R_0 = N, R_1 = D$ . Tant que  $R_i$  est non nul, on pose :

$$R_{i+1} = R_{i-1} \text{ mod } R_i .$$

Ainsi,  $\text{pgcd}(R_i, R_{i+1})$  est un invariant.

En outre,  $\text{deg } R_{i+1} < \text{deg } R_i$  pour  $i \geq 1$ . L'algorithme se termine donc au bout d'un nombre fini d'étapes.

De plus, si  $R_n$  est le dernier reste non nul, on a :

$$\text{pgcd}(R_n, R_{n+1}) = \text{pgcd}(R_n, 0) = R_n ,$$

donc  $\text{pgcd}(N, D) = R_n$  :

$$\boxed{\text{le pgcd est le dernier reste non nul}} .$$

De plus,  $n \leq \text{deg } R_1 = \text{deg } D$ . Le nombre de divisions successives est inférieur ou égal à  $\text{deg } D$ .

Bien entendu, par une comparaison des degrés, on peut choisir  $D$  de telle sorte que :

$$\text{deg } D = \min(\text{deg } N, \text{deg } D) .$$

**Exemple** : Le corps de base est  $\mathbb{Q}$ . On cherche le pgcd des polynômes :

$$N = X^6 + X^5 + X^4 - 2X^2 - 2X - 2$$

$$D = X^4 - X^2 - 2X - 1$$

• Division euclidienne de  $R_0 = N$  par  $R_1 = D$  :

$$R_0 = (X^2 + X + 2)R_1 + R_2 , \text{ avec } R_2 = 3X^3 + 3X^2 + 3X .$$

• Division euclidienne de  $R_1$  par  $R_2$  :

$$R_1 = \frac{X-1}{3}R_2 + R_3 , \text{ avec } R_3 = -X^2 - X - 1$$

• Division euclidienne de  $R_2$  par  $R_3$  :

$$R_2 = -3X R_3 + R_4 , \text{ avec } R_4 = 0 .$$

Donc  $\Delta = \text{pgcd}(N, D) = -R_3 = X^2 + X + 1$

(on a pris un pgcd de coefficient dominant égal à 1).

En détaillant les calculs, on peut obtenir un couple de coefficients de Bezout.

Initialisons :

$$M_0 = \begin{pmatrix} 1 & 0 & N \\ 0 & 1 & D \end{pmatrix} \quad R_0 = N ; R_1 = D .$$

Tant que  $R_i \neq 0$ , posons  $R_{i-1} = R_i Q_i + R_{i+1}$  (division euclidienne).

On peut écrire :  $R_0 = U_0 N + V_0 D$  et si, par récurrence :

$$R_i = U_i N + V_i D ,$$

alors :

$$R_{i+1} = U_{i-1}N + V_{i-1}D - U_i Q_i N - V_i Q_i D$$

$$R_{i+1} = (U_{i-1} - U_i Q_i)N + (V_{i-1} - V_i Q_i)D = U_{i+1}N + V_{i+1}D$$

Introduisons la matrice :  $P_i = \begin{pmatrix} 0 & 1 \\ 1 & -Q_i \end{pmatrix}$ . Ainsi :

$$\begin{pmatrix} U_i & V_i & R_i \\ U_{i+1} & V_{i+1} & R_{i+1} \end{pmatrix} = P_i \begin{pmatrix} U_{i-1} & V_{i-1} & R_{i-1} \\ U_i & V_i & R_i \end{pmatrix}$$

ou encore :  $M_i = P_i M_{i-1}$ .

En particulier, si  $R_n \neq 0$  et  $R_{n+1} = 0$ , on aura :

$$R_n = \text{pgcd}(N, D) = U_n N + V_n D .$$

L'algorithme peut se reformuler ainsi :

$$M_0 = \begin{pmatrix} 1 & 0 & N \\ 0 & 1 & D \end{pmatrix} ; R_0 = N ; R_1 = D .$$

Tant que  $R_i \neq 0$ , soit  $Q_i$  le quotient euclidien de  $R_{i-1}$  par  $R_i$ .

Alors :

$$\begin{pmatrix} U_i & V_i & R_i \\ U_{i+1} & V_{i+1} & R_{i+1} \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -Q_i \end{bmatrix} \begin{pmatrix} U_{i-1} & V_{i-1} & R_{i-1} \\ U_i & V_i & R_i \end{pmatrix}$$

$$\boxed{\text{Résultat : } R_n = \text{pgcd}(N, D) \\ R_n = U_n N + V_n D .}$$

**Complexité de l'algorithme d'Euclide.** Il se trouve que, parmi les algorithmes de calcul de pgcd n'utilisant que des divisions euclidiennes, l'algorithme d'Euclide précédent est optimal. Dans le pire des cas, il nécessite  $(1 + \text{deg } D)$  divisions euclidiennes.

**■ Factorialité de  $\mathbb{K}[X]$**

Notons  $\mathcal{P}$  l'ensemble des polynômes **irréductibles** de  $\mathbb{K}[X]$  qui sont unitaires. Tout polynôme irréductible est ainsi associé à un polynôme de  $\mathcal{P}$ .

Le fait que  $\mathbb{K}[X]$  est principal a pour conséquence la **factorialité** de  $\mathbb{K}[X]$  : tout polynôme  $Q$  non nul de  $\mathbb{K}[X]$  peut s'écrire :

$$Q = \lambda \prod_{P \in \mathcal{P}} P^{\alpha_P}$$

où  $\lambda$  est un élément non nul de  $\mathbb{K}$ ,  $\alpha_P$  un entier naturel, les  $\alpha_P$  étant nuls sauf pour un nombre fini de polynômes  $P$  (ce qui est rappelé par le symbole  $\prod'$ , qui indique que le produit porte sur un nombre fini de polynômes).

En outre, cette écriture est unique. En d'autres termes, la famille  $(\alpha_P)_{P \in \mathcal{P}}$  ne dépend que de  $Q$ .

On note :  $\alpha_P = v_P(Q)$ . Cet entier est appelé **valuation P-adique** de  $Q$ .

On peut donc écrire :

$$Q = \lambda \prod_{P \in \mathcal{P}} P^{v_P(Q)}$$

Notons que  $\lambda$  n'est rien d'autre que le coefficient dominant de  $Q$ .

Il est facile de caractériser la **relation de divisibilité**. Si  $Q_1$  et  $Q_2$  sont deux polynômes non nuls, on a :

$$Q_1 | Q_2 \Leftrightarrow \forall P \in \mathcal{P} \quad v_P(Q_1) \leq v_P(Q_2)$$

On peut aussi calculer le pgcd d'une famille  $(Q_i)$  de polynômes non nuls :

$$\forall P \in \mathcal{P} \quad v_P(\text{pgcd}(Q_i)) = \min_{i \in I} v_P(Q_i)$$

Cette méthode est plus théorique que pratique. En effet, la détermination de  $v_P(Q)$  est un problème difficile.

**■ ppcm d'une famille de polynômes**

Soit  $(Q_i)_{i \in I}$  une famille de polynômes. L'idéal  $\bigcap_{i \in I} Q_i \mathbb{K}[X]$  est un idéal principal de  $\mathbb{K}[X]$ . Un générateur  $\mu$  de cet idéal est appelé **plus petit commun multiple** de la famille  $(Q_i)_{i \in I}$ . On note :

$$\mu = \text{ppcm}(Q_i)_{i \in I}$$

On le choisira souvent unitaire, lorsque  $\bigcap_{i \in I} Q_i \mathbb{K}[X] \neq \{0\}$ .

Un polynôme  $\mu$  est caractérisé par la double condition :

$$\forall i \in I \quad \mu | Q_i ;$$

si  $\forall i \in I \quad m | Q_i$ , alors  $\mu | m$ .

Un ppcm de la famille  $(Q_i)_{i \in I}$  est donc un plus petit élément (pour la relation de divisibilité) de l'ensemble des diviseurs communs aux  $Q_i$ . C'est, dans le cas particulier où  $I$  est un ensemble fini, un diviseur de  $\prod_{i \in I} Q_i$ .

Notons aussi qu'un ppcm de la famille  $(Q_i)_{i \in I}$  est un polynôme de plus petit degré qui divise tous les  $Q_i$ .

Pour calculer le ppcm de la famille  $(Q_i)_{i \in I}$ , où  $I$  est fini ( $I = \{1, n\}$ ), on utilise l'associativité du ppcm :

$$\text{ppcm}(Q_1, \dots, Q_n) = \text{ppcm}(\text{ppcm}(Q_1, \dots, Q_{n-1}), Q_n)$$

de façon à se ramener à deux polynômes non nuls  $Q_1$  et  $Q_2$ .

On utilise ensuite la formule :

$$\text{pgcd}(Q_1, Q_2) \cdot \text{ppcm}(Q_1, Q_2) = Q_1 Q_2$$

qui résulte de l'égalité :

$$\begin{aligned} \forall P \in \mathcal{P} \quad \min(v_P(Q_1), v_P(Q_2)) + \max(v_P(Q_1), v_P(Q_2)) \\ = v_P(Q_1) + v_P(Q_2) \end{aligned}$$

De cette façon, le calcul du ppcm se ramène au calcul du pgcd, que l'on obtient à l'aide de l'algorithme d'Euclide.

**Exemple :** Reprenons l'exemple de :

$$N = X^6 + X^5 + X^4 - 2X^2 - 2X - 2 \quad \text{et} \quad D = X^4 - X^2 - 2X - 1$$

On a vu que  $\Delta = \text{pgcd}(N, D) = X^2 + 1$ .

Il en résulte que :

$$\text{ppcm}(N, D) = \frac{ND}{\Delta} = N \frac{D}{\Delta}$$

Une division euclidienne fournit :

$$\frac{D}{\Delta} = X^2 - X - 1$$

Ainsi :

$$\text{ppcm}(N, D) = (X^6 + X^5 + X^4 - 2X^2 - 2X - 2)(X^2 - X - 1)$$

**1.3.3.3 Étude de  $\mathbb{A}[X]$  ( $\mathbb{A}$  anneau factoriel)**

On suppose dans tout ce paragraphe que  $\mathbb{A}$  est un anneau **factoriel**.

On notera  $\mathcal{P}$  une famille représentative des irréductibles de  $\mathbb{A}$ , c'est-à-dire telle que tout irréductible de  $\mathbb{A}$  est associé à un élément et un seul de la famille  $\mathcal{P}$ .

On notera aussi  $U(\mathbb{A})$  le groupe des inversibles de  $\mathbb{A}$ .

Rappelons que, par définition, un anneau factoriel est aussi intègre.

**Définition 3.** Soient  $Q \in \mathbb{A}[X]$  et  $Q = \sum_{i \in \mathbb{N}} q_i X^i$ . On appelle contenu de  $Q$ , et on note  $c(Q)$ , un pgcd de la famille  $(q_i)_{i \in I}$ .

**Exemple :** ①  $\mathbb{A} = \mathbb{Z}$  ;  $Q = 6X^3 + 2X - 4$ .

On a alors :  $c(Q) = 2$ .

②  $\mathbb{A} = \mathbb{Q}[X_1]$  ;  $Q = X_1^2 X^3 + 2X_1 X^2 + 3X_1^4 X$ .

Dans  $\mathbb{Q}[X_1]$ ,  $\text{pgcd}(X_1^2, 2X_1, 3X_1^4) = X_1$ .

Donc :  $c(Q) = X_1$ .

Bien entendu,  $c(Q)$  n'est pas unique : deux contenus sont associés.

Nous disposons des propriétés suivantes :

①  $c(Q) = 0 \Leftrightarrow Q = 0$  ;

② si  $\lambda \in \mathbb{A}$ , alors  $c(\lambda Q) = \lambda c(Q)$  ;

③ si  $\lambda$  divise tous les coefficients de  $Q$ , on peut écrire :

$$Q = \lambda Q_1 \quad \text{où} \quad Q_1 \in \mathbb{A}[X] ;$$

④ en particulier, pour tout polynôme  $Q$ , on peut écrire :

$$Q = c(Q) Q_1$$

En outre,  $c(Q) = c(Q) c(Q_1)$  d'après la propriété ③.

Si donc  $Q \neq 0$ , on a :  $c(Q_1) = 1$ .

On appelle polynôme **primitif** un polynôme de contenu égal à 1. Tout polynôme peut donc s'écrire sous la forme :

$$Q = c(Q) Q_1,$$

où  $Q_1$  est un polynôme primitif (dans le cas où  $Q = 0$ ,  $Q_1$  n'est pas unique, mais on peut toujours prendre  $Q_1 = 1$ ).

**Proposition 9.**

Soient  $Q$  et  $S$  deux polynômes de  $\mathbb{A}[X]$ . Alors :

$$c(QS) = c(Q) c(S)$$

**Preuve.** ♦ Puisque  $\mathbb{A}[X]$  est intègre, la propriété est vraie lorsque  $Q$  ou  $S$  est nul.

Supposons à présent ces polynômes non nuls. On peut écrire :

$$Q = c(Q) Q_1 \text{ et } S = c(S) S_1,$$

où  $Q_1$  et  $S_1$  sont de contenu 1. Alors :

$$QS = c(Q) c(S) Q_1 S_1$$

et  $c(QS) = c(Q) c(S) c(Q_1 S_1)$ .

Tout revient donc à montrer que  $Q_1 S_1$  est primitif lorsque  $Q_1$  et  $S_1$  le sont.

Soit  $p \in \mathcal{P}$ . On sait que l'anneau quotient  $\mathbb{A}/p\mathbb{A}$  est intègre.

Notons  $\bar{Q} \in \mathbb{A}/p\mathbb{A}[X]$  le polynôme  $\sum_{i \in I} \bar{q}_i X^i$ , lorsque  $Q = \sum_{i \in I} q_i X^i$

et lorsque  $\bar{q}_i$  désigne la classe de  $q_i$  dans  $\mathbb{A}/p\mathbb{A}$ . On obtient alors :

$$\bar{Q}_1 \bar{S}_1 = \overline{Q_1 S_1}$$

Mais  $\bar{Q}_1 \neq \bar{0}$  car  $p$  ne divise pas tous les coefficients de  $Q_1$ . De même  $\bar{S}_1 \neq \bar{0}$ . Comme  $\mathbb{A}/p\mathbb{A}[X]$  est intègre,  $\bar{Q}_1 \bar{S}_1 \neq \bar{0}$ . En particulier,  $c(Q_1 S_1)$  n'est divisible par aucun irréductible de  $\mathbb{A}$ . C'est donc un inversible de  $\mathbb{A}$  et :  $c(Q_1 S_1) = 1$ . ♦

Cette proposition 9 est due à Gauss.

Considérons le corps des fractions  $\mathbb{K}$  de l'anneau intègre  $\mathbb{A}$ . Tout élément de  $\mathbb{A}[X]$  peut donc être considéré comme un élément de  $\mathbb{K}[X]$ . Nous allons caractériser les polynômes irréductibles de  $\mathbb{A}[X]$  à l'aide des éléments irréductibles de  $\mathbb{A}$  et des polynômes irréductibles de  $\mathbb{K}[X]$ .

**Proposition 10.**

Soit  $P \in \mathbb{A}[X] - \mathbb{A}$  où  $\mathbb{A}$  est un anneau factoriel.

Il y a équivalence entre :

- ①  $P$  est un irréductible de  $\mathbb{A}[X]$  ;
- ②  $P$  est primitif et  $P$  est un irréductible de  $\mathbb{K}[X]$ .

**Preuve.** ♦

①  $\Rightarrow$  ②

Puisque  $P = c(P) P_1$ , où  $P_1 \in \mathbb{A}[X]$ , on a nécessairement  $c(P) \in U(\mathbb{A})$ .

Supposons que  $P$  puisse s'écrire :

$$P = QS$$

où  $Q \in \mathbb{K}[X]$  et  $S \in \mathbb{K}[X]$ .

Un polynôme  $Q$  de  $\mathbb{K}[X]$  peut s'écrire, après réduction à un dénominateur commun :

$$Q = \frac{1}{\lambda} Q_1 \text{ où } Q_1 \in \mathbb{A}[X], \quad \lambda \in \mathbb{A}.$$

Soit :  $Q = \frac{\mu}{\lambda} Q_2$  où  $Q_2 \in \mathbb{A}[X]$ ,  $Q_2$  est primitif,

et où  $\text{pgcd}(\mu, \lambda) = 1$  (c'est-à-dire que l'on a pris une forme irréductible de la fraction  $\frac{c(Q_1)}{\lambda}$ ).

De même :  $S = \frac{\alpha}{\beta'} S_2$ , avec  $S_2$  primitif et  $\text{pgcd}(\alpha, \beta') = 1$ .

Donc :

$$P = QS = \frac{\alpha\mu}{\lambda'\beta'} Q_2 S_2$$

ou encore

$$\lambda' \beta' P = \alpha\mu Q_2 S_2.$$

Il en résulte :

$$\lambda' \beta' = \alpha\mu c(Q_2 S_2) = \alpha\mu.$$

Mais  $\text{pgcd}(\lambda' \beta', \alpha\mu) = 1$ . Donc :  $\lambda' \beta' \in U(\mathbb{A})$  et  $\alpha\mu \in U(\mathbb{A})$ .

Ainsi :  $P = k Q_2 S_2$  où  $k \in U(\mathbb{A})$ .

Puisque  $P$  est irréductible dans  $\mathbb{A}[X]$ , on a, par exemple,  $\text{deg } Q_2 = 0$ .

Donc  $\text{deg } Q = 0$ , et  $Q$  est inversible dans  $\mathbb{K}$ .

②  $\Rightarrow$  ① Supposons que  $P$  puisse s'écrire :

$$P = QS$$

où  $Q \in \mathbb{A}[X]$  et  $S \in \mathbb{A}[X]$ . Puisque  $P, Q, S$  sont dans  $\mathbb{K}[X]$ , on a, par exemple,  $\text{deg } Q = 0$ . Donc  $Q \in \mathbb{A}$  ; notons  $Q = \lambda$ . Alors  $c(P) = \lambda c(S)$ . Comme  $\lambda$  divise un inversible de  $\mathbb{A}$ ,  $\lambda$  est inversible. Cela prouve finalement que  $Q$  est irréductible. ♦

La proposition 10 caractérise les polynômes non constants de  $\mathbb{A}[X]$  qui sont irréductibles dans  $\mathbb{A}[X]$  ; quant aux polynômes constants, il est facile de voir qu'ils sont irréductibles si, et seulement si, ils sont irréductibles comme éléments de  $\mathbb{A}$ .

**Théorème 4.** Si  $\mathbb{A}$  est un anneau factoriel, alors  $\mathbb{A}[X]$  est encore factoriel.

**Preuve.** ♦ Soit  $R$  un élément de  $\mathbb{K}[X]$ . On peut toujours écrire :

$$R = \frac{\lambda}{\mu} S, \text{ où } (\lambda, \mu) \in \mathbb{A}^2 \text{ et } S \in \mathbb{A}[X].$$

On peut, en outre, supposer  $c(S) = 1$ . Si, de plus,  $R$  est irréductible dans  $\mathbb{K}[X]$ ,  $S$  est aussi irréductible dans  $\mathbb{K}[X]$ , car il est associé (dans  $\mathbb{K}[X]$ ) à  $R$ . Donc  $S$ , étant primitif, est irréductible dans  $\mathbb{A}[X]$ .

■ **Existence d'une décomposition en facteurs irréductibles dans  $\mathbb{A}[X]$**

Soit  $Q \in \mathbb{A}[X]$ . C'est un produit d'irréductibles de  $\mathbb{K}[X]$ , car  $\mathbb{K}[X]$  est principal (§ 1.3.3.2), donc factoriel. Par conséquent, on peut écrire :

$$Q = \frac{\alpha}{\beta} Q_1$$

où  $(\alpha, \beta) \in \mathbb{A}^2$  et  $Q_1$  est un produit d'irréductibles de  $\mathbb{A}[X]$ .

En particulier,  $c(Q_1) = 1$ , donc  $\alpha = \beta c(Q)$ . Ainsi,  $\frac{\alpha}{\beta} \in \mathbb{A}$ . Puisque  $\mathbb{A}$

est factoriel,  $\frac{\alpha}{\beta}$  est un produit d'irréductibles de  $\mathbb{A}$ , donc, évidemment, de  $\mathbb{A}[X]$ .

L'existence d'une décomposition est ainsi assurée.

■ **Unicité d'une décomposition en facteurs irréductibles dans  $\mathbb{A}[X]$**

Supposons l'égalité :

$$Q = \prod_{i \in I} P_i^{\alpha_i}$$

où les  $P_i$  sont des irréductibles de  $\mathbb{A}[X]$ . On peut écrire :

$$Q = a \prod_{i \in I} P_i^{\alpha_i}$$

où  $a$  désigne le produit  $\prod_{i \in I-J} P_i^{\alpha_i}$ , les éléments  $P_i$  intervenant dans ce produit correspondant aux polynômes constants, c'est-à-dire aux éléments de  $\mathbb{A}$ . D'après l'unicité d'une décomposition dans  $\mathbb{K}[X]$ , on a nécessairement lorsque  $v_{P_i}$  désigne la valuation  $P_i$ -adique dans  $\mathbb{K}[X]$  :

$$\alpha_i = v_{P_i}(Q)$$

puisque  $P_i$  est aussi un irréductible de  $\mathbb{K}[X]$ . De plus :

$$c(Q) = a$$

car  $c(P_i) = 1$ . Donc  $\prod_{i \in I-J} P_i^{\alpha_i}$  est une décomposition de  $a$  en facteurs irréductibles dans  $\mathbb{A}$ , décomposition unique d'après la factoriabilité de  $\mathbb{A}$ . L'unicité est ainsi montrée.  $\diamond$

On peut donc appliquer, dans  $\mathbb{A}[X]$ , les règles usuelles de l'arithmétique, pour autant qu'elles relèvent de la factoriabilité. Cependant, l'égalité de Bezout, et plus généralement les propriétés liées à la principalité, ne sont plus vérifiées en général dans  $\mathbb{A}[X]$ .

### 1.4 Polynômes symétriques, antisymétriques de $\mathbb{A}[X_1, \dots, X_n]$

**Définition 4.** Soient  $\sigma \in S_n$ , groupe des permutations de  $[1, n]$ , et  $P \in \mathbb{A}[X_1, \dots, X_n]$ . On pose :

$$P_\sigma = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

① Le polynôme  $P$  est dit **symétrique** lorsque :

$$\forall \sigma \in S_n \quad P_\sigma = P$$

② Le polynôme  $P$  est dit **antisymétrique** lorsque :

$$\forall \sigma \in S_n \quad P_\sigma = \varepsilon(\sigma)P$$

Rappelons que  $\varepsilon(\sigma)$  désigne la **signature** de  $\sigma$ ;  $\varepsilon(\sigma)$  vaut 1 ou -1, selon que  $\sigma$  est une permutation paire ou impaire.

**Exemple :** Soit :

$$V = \begin{vmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_n \\ \vdots & \vdots & \dots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \dots & X_n^{n-1} \end{vmatrix} \in \mathbb{A}[X_1, \dots, X_n]$$

Les propriétés du déterminant prouvent que  $V$  est antisymétrique. Ce polynôme est appelé **polynôme de Vandermonde**. On peut l'expliciter :

$$V = \prod_{n \geq i > j \geq 1} (X_i - X_j)$$

C'est un polynôme homogène, de degré  $\frac{(n-1)n}{2}$ . On a aussi :

$$\deg_{X_i} V = n - 1$$

#### Proposition 11.

Soit  $\mathbb{A}$  un anneau, de caractéristique différente de 2.

Soit  $P \in \mathbb{A}[X_1, \dots, X_n]$ . Il y a équivalence entre :

①  $P$  est antisymétrique.

② Il existe  $T$  symétrique tel que :

$$P = VT$$

**Preuve.**  $\diamond$

②  $\Rightarrow$  ① On a, d'après les propriétés de la substitution (§ 1.1.3) :

$$P_\sigma = V_\sigma Q_\sigma = \varepsilon(\sigma) VQ = \varepsilon(\sigma)P$$

①  $\Rightarrow$  ② Considérons  $P \in \mathbb{A}[X_1, \dots, X_{n-1}][X_n]$  et

$$S = (X_n - X_1) \dots (X_n - X_{n-1}) \in \mathbb{A}[X_1, \dots, X_{n-1}][X_n]$$

Puisque le coefficient dominant de  $S$  est 1, on peut appliquer le théorème 2 et diviser  $P$  par  $S$  :

$$P = SQ + R ; \deg_{X_n} R \leq n - 2$$

Pour  $i \in [1, n - 1]$ , on a :

$$P(X_1, \dots, X_i, \dots, X_{n-1}, X_i) = -P(X_1, \dots, X_i, \dots, X_{n-1}, X_i)$$

car  $P_\tau = -P_\tau$ , où  $\tau$  est la transposition  $(i, n)$ .

$$\text{Donc : } P(X_1, \dots, X_i, \dots, X_{n-1}, X_i) = 0$$

Il en résulte que :

$$R(X_1, \dots, X_i, \dots, X_{n-1}, X_i) = 0$$

puisque  $S(X_1, \dots, X_i, \dots, X_{n-1}, X_i) \neq 0$ .

Le polynôme  $R$ , considéré comme un élément de  $\mathbb{A}[X_1, \dots, X_{n-1}][X_n]$ , admet les  $(n - 1)$  racines  $X_1, \dots, X_{n-1}$ . Comme il est de degré inférieur ou égal à  $(n - 2)$ , il est nul. Ainsi :

$$P = SQ$$

Soit  $\sigma$  une permutation telle que  $\sigma(n) = n$ . On a :

$$P_\sigma = S$$

Donc :  $Q_\sigma = \varepsilon(\sigma) Q$ .

On peut appliquer une hypothèse de récurrence à  $Q \in \mathbb{A}[X_n][X_1, \dots, X_{n-1}]$ , antisymétrique par rapport aux  $(n - 1)$  dernières indéterminées. Ainsi, il existe  $T$  tel que :

$$Q = V_1 T$$

avec  $V_1 = \prod_{n-1 \geq i > j \geq 1} (X_i - X_j)$ . Donc :

$$P = SV_1 T = VT$$

De plus :

$$V_\sigma T_\sigma = P_\sigma = -P \Rightarrow VT_\sigma = VT \Rightarrow T_\sigma = T$$

Donc  $T$  est nécessairement symétrique.  $\diamond$

Grâce à la proposition 11, l'étude des polynômes antisymétriques se ramène, lorsque la caractéristique de  $\mathbb{A}$  est différente de 2, à l'étude des polynômes symétriques. Lorsque  $\mathbb{A}$  est de caractéristique 2, on a  $-P = P$ , donc les polynômes antisymétriques et symétriques sont les mêmes.

Nous introduisons les polynômes **symétriques élémentaires**  $S_1, \dots, S_n$  suivants :

$$S_1 = X_1 + \dots + X_n = \sum_{i=1}^n X_i$$

$$S_2 = X_1 X_2 + \dots + X_1 X_n + X_2 X_3 + \dots + X_2 X_n + \dots + X_{n-1} X_n$$

soit  $S_2 = \sum_{1 \leq i_1 < i_2 \leq n} X_{i_1} X_{i_2}$

et, plus généralement :

$$S_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} X_{i_1} X_{i_2} \dots X_{i_k}$$

Ainsi :

$$\begin{aligned} S_{n-1} &= X_1 X_2 \dots X_{n-1} + X_1 X_2 \dots X_{n-2} X_n + \dots + X_2 X_3 \dots X_n \quad ; \\ S_n &= X_1 X_2 \dots X_n . \end{aligned}$$

**Proposition 12.**

On a, dans  $\mathbb{A}[X_1, \dots, X_n][T]$  :

$$(T - X_1)(T - X_2) \dots (T - X_n) = T^n - S_1 T^{n-1} + S_2 T^{n-2} + \dots + (-1)^k S_k T^{n-k} + \dots + (-1)^n S_n .$$

Cette proposition résulte d'un simple calcul. Évaluée en un  $n$ -uplet  $(x_1, \dots, x_n)$  de  $\mathbb{A}$ , l'égalité précédente permet d'exprimer les coefficients  $-s_1, s_2, \dots, (-1)^k s_k, \dots, (-1)^n s_n$  d'un polynôme de  $\mathbb{A}[T]$ , connaissant la liste  $(x_1, \dots, x_n)$  de ses racines.

Pour cette raison, on parle souvent de **fonctions symétriques élémentaires des racines**.

Il est clair que  $S_1, \dots, S_n$  sont des polynômes symétriques de  $\mathbb{A}[X_1, \dots, X_n]$  : il suffit de substituer  $(X_{\sigma(1)}, \dots, X_{\sigma(n)})$  à  $(X_1, \dots, X_n)$  dans le membre de gauche de l'égalité qui précède. De plus,  $S_k$  est un polynôme homogène de degré  $k$ , qui est de degré 1 par rapport à chacun des  $X_j$ .

Soit  $U$  un polynôme en  $n$  indéterminées, à coefficients dans  $\mathbb{A}$ . Le polynôme  $U(S_1, \dots, S_n)$  est manifestement un polynôme symétrique de  $\mathbb{A}[X_1, \dots, X_n]$ .

Le théorème ci-dessous affirme que la réciproque est vraie.

**Théorème 5.** Soit  $P \in \mathbb{A}[X_1, \dots, X_n]$ , symétrique. Il existe un unique polynôme  $U$ , à  $n$  indéterminées et à coefficients dans  $\mathbb{A}$ , tel que  $P = U(S_1, \dots, S_n)$ .

**Preuve.** Sur les monômes  $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ , on met l'ordre lexicographique  $(\alpha_1, \dots, \alpha_n) \geq (\beta_1, \dots, \beta_n)$  défini par :

$$\alpha_1 > \beta_1 \text{ ou } ((\alpha_1 = \beta_1 \text{ et } \alpha_2 > \beta_2) \dots \text{ ou } (\alpha_n \geq \beta_n) \dots) .$$

Pour cet ordre, cherchons le plus grand monôme de  $S_k$  : c'est manifestement  $X_1 \dots X_k$ .

Le plus grand monôme de  $S_1^{\beta_1} S_2^{\beta_2} \dots S_n^{\beta_n}$  est donc :

$$X_1^{\beta_1 + \dots + \beta_n} X_2^{\beta_2 + \dots + \beta_n} \dots X_n^{\beta_n} .$$

■ **Unicité**

Par différence, il s'agit de montrer que si :

$$P(X_1, \dots, X_n) = Q(S_1, \dots, S_n) = 0$$

dans  $\mathbb{A}[X_1, \dots, X_n]$ ,  $Q$  est le polynôme nul. Supposons le contraire,

et soit  $\lambda$  le coefficient non nul de  $S_1^{\beta_1} \dots S_n^{\beta_n}$ , où  $(\beta_1, \dots, \beta_n)$  est choisi de telle façon que  $(\beta_1 + \dots + \beta_n, \beta_2 + \dots + \beta_n, \dots, \beta_n)$  soit maximal pour l'ordre lexicographique introduit ci-dessus. Il faut seulement remarquer qu'il existe un unique tel monôme, car la donnée de  $(\beta_1 + \dots + \beta_n, \dots, \beta_n)$  détermine celle de  $(\beta_1, \dots, \beta_n)$ . On voit alors que  $\lambda$  est le coefficient du plus grand monôme de  $P$ , donc est nul : d'où la contradiction.

■ **Existence**

Soit  $\lambda X_1^{\alpha_1} \dots X_n^{\alpha_n}$  le plus grand monôme de  $P \in \mathbb{A}[X_1, \dots, X_n]$ , avec  $\lambda \neq 0$ .

Il est certain que  $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$ . En effet, on a, pour toute permutation  $\sigma \in S_n$  :

$$(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) \leq (\alpha_1, \dots, \alpha_n) ,$$

puisque  $\lambda X_{\sigma(1)}^{\alpha_1} \dots X_{\sigma(n)}^{\alpha_n}$  figure aussi dans l'expression de  $P$ .

On peut alors déterminer des entiers naturels  $\beta_1, \dots, \beta_n$  tels que :

$$\beta_1 + \dots + \beta_n = \alpha_1 ; \dots ; \beta_n = \alpha_n .$$

Le polynôme  $R - \lambda S_1^{\beta_1} \dots S_n^{\beta_n}$  est encore symétrique, et son monôme maximal est strictement inférieur à  $(\alpha_1, \dots, \alpha_n)$ .

On conclut alors par une hypothèse de récurrence (qui utilise le fait que l'ordre lexicographique est un bon ordre sur  $\mathbb{N}^n$ ). ◊

La démonstration précédente est constructive.

$$P = X_1^3 + X_2^3 + X_3^3 - X_1^2 X_2 - X_1 X_2^2 - X_2^2 X_3 - X_1 X_2^2 - X_1 X_3^2 - X_2 X_3^2 .$$

Le monôme maximal est  $X_1^3$ . On a :

$$\begin{aligned} S_1^3 &= X_1^3 + X_2^3 + X_3^3 \\ &\quad + 3(X_1^2 X_2 + X_1^2 X_3 + X_2^2 X_3 + X_1 X_2^2 + X_1 X_3^2 + X_2 X_3^2) + 6X_1 X_2 X_3 \end{aligned}$$

Donc :

$$P - S_1^3 = -4(X_1^2 X_2 + X_1^2 X_3 + X_2^2 X_3 + X_1 X_2^2 + X_1 X_3^2 + X_2 X_3^2) - 6X_1 X_2 X_3$$

Le plus grand monôme est ensuite  $-4 X_1^2 X_2$ . On calcule :

$$S_1 S_2 = (X_1 + X_2 + X_3)(X_1 X_2 + X_1 X_3 + X_2 X_3)$$

Donc :

$$P - S_1^3 + 4 S_1 S_2 = 6 X_1 X_2 X_3 .$$

Enfin,  $X_1 X_2 X_3 = S_3$ . D'où :

$$P = S_1^3 - 4 S_1 S_2 + 6 S_3 .$$

## 2. Polynômes irréductibles

Puisque, lorsque l'anneau  $\mathbb{A}$  est factoriel, l'étude de la divisibilité se ramène à la décomposition d'un polynôme en facteurs irréductibles, il est essentiel de pouvoir déterminer les polynômes irréductibles d'un anneau de polynômes. Cette question ne peut pas être abordée sans une connaissance préalable de  $\mathbb{A}$ . Très souvent,  $\mathbb{A}$  sera d'ailleurs un corps. Nous discuterons donc des polynômes irréductibles en relation étroite avec l'anneau  $\mathbb{A}$ .

### 2.1 Racines d'un élément de $\mathbb{K}[X]$

Dans ce paragraphe 2.1,  $\mathbb{K}$  désigne un corps.

#### 2.1.1 Corps algébriquement clos

Dans  $\mathbb{K}[X]$ , un polynôme de degré 1 est toujours irréductible, car un diviseur non constant est aussi de degré 1, donc est associé au polynôme initial.

**Définition 5.** On dit qu'un corps est algébriquement clos lorsque les polynômes irréductibles sont ceux de degré un.

Autrement dit, il n'y a pas d'autre polynôme irréductible que ceux qui sont de degré 1.

**Proposition 13.**

Soit  $\mathbb{K}$  un corps. Les propriétés suivantes sont équivalentes :

- ①  $\mathbb{K}$  est algébriquement clos ;
- ② tout polynôme  $P$  de  $\mathbb{K}[X]$ , non constant, admet au moins une racine ;
- ③ tout polynôme  $P$  de  $\mathbb{K}[X]$ , non nul, peut s'écrire :

$$\lambda \prod_{\alpha \in \mathbb{K}} (X - \alpha)^{m(\alpha)} \quad \text{où } m(\alpha) \in \mathbb{N} \text{ et } \lambda \in \mathbb{K} - \{0\} .$$

**Preuve.** ◊

① ⇒ ③ :  $P$  admet une décomposition en facteurs irréductibles unitaires, de la forme  $X - \alpha$ ,  $\alpha \in \mathbb{K}$ . Le nombre  $m(\alpha)$  n'est rien d'autre que la valuation  $(X - \alpha)$ -adique de  $P$ .

③ ⇒ ② est clair, car  $\deg P = \sum_{\alpha \in \mathbb{K}} m(\alpha)$ , donc au moins un des  $m(\alpha)$  est supérieur ou égal à 1.

② ⇒ ① : si  $P$  est irréductible (donc non constant), il admet une racine  $\alpha$ , donc est associé à  $X - \alpha$ . Il est par conséquent de degré 1. ◊

Un exemple fondamental est donné par le théorème suivant.

**Théorème 6.** Le corps  $\mathbb{C}$  des nombres complexes est algébriquement clos.

**Preuve.** ◊ Soit  $P \in \mathbb{C}[X]$ , non constant. On a :

$$|P(z)| \rightarrow +\infty \quad \text{quand } |z| \rightarrow +\infty$$

Si, par l'absurde,  $P$  ne s'annule pas dans  $\mathbb{C}$ , l'application  $z \mapsto \frac{1}{P(z)}$ , continue et tendant vers 0 à l'infini, est bornée sur  $\mathbb{C}$ . Comme elle est holomorphe, elle est constante sur  $\mathbb{C}$ , ce qui est une contradiction. ◊

Ce théorème explique l'usage fréquent que l'on fait du corps des complexes pour des calculs qui, a priori, sont destinés à des polynômes à coefficients réels.

Abstraitement, on peut plonger un corps quelconque dans un corps algébriquement clos.

**Théorème 7.** Soit  $\mathbb{K}$  un corps. Il existe un sur-corps  $\mathbb{L}$  de  $\mathbb{K}$  qui est algébriquement clos.

La construction générale de ce corps  $\mathbb{L}$  n'est pas effective bien que, dans certains cas particuliers, un tel corps  $\mathbb{L}$  puisse être explicité : par exemple, lorsque  $\mathbb{K} = \mathbb{R}$  et  $\mathbb{L} = \mathbb{C}$ .

**2.1.2 Multiplicité des racines**

Soit  $\alpha \in \mathbb{K}$ . On note  $m(\alpha)$  la valuation  $(X - \alpha)$ -adique du polynôme  $P$  de  $\mathbb{K}[X]$ , supposé non nul. Ainsi,  $m(\alpha)$  est la plus grande puissance de  $X - \alpha$  qui divise  $P$ . Bien entendu, en général,  $\alpha$  n'est pas racine de  $P$ , ce qui signifie que  $m(\alpha) = 0$ .

Lorsque  $m(\alpha) = 1$ , on dit que  $\alpha$  est **racine simple** de  $P$ .

Lorsque  $m(\alpha) \geq 2$ , on dit que  $\alpha$  est **racine multiple** de  $P$  : double lorsque  $m(\alpha) = 2$ , triple lorsque  $m(\alpha) = 3$ , etc.

De façon générale,  $m(\alpha)$  est appelé **ordre de multiplicité** de  $\alpha$  dans  $P$ .

**Proposition 14.**

Soit  $P \in \mathbb{K}[X] - \{0\}$ . Il y a équivalence entre :

- ①  $m(\alpha) \geq 2$  ;
- ②  $P(\alpha) = P'(\alpha) = 0$ .

**Preuve.** ◊

① ⇒ ② Si  $P = (X - \alpha)^2 Q$ , on a :

$$P' = 2(X - \alpha)Q + (X - \alpha)^2 Q' .$$

Donc :  $P(\alpha) = P'(\alpha) = 0$ .

② ⇒ ①. Si  $P(\alpha) = 0$ , on peut écrire :

$$P = (X - \alpha)R$$

avec  $P' = (X - \alpha)R' + R$ , donc  $R(\alpha) = 0$ . Ainsi,  $R$  est divisible par  $X - \alpha$ . ◊

Pour déterminer  $m(\alpha)$  de façon générale, remarquons que la famille  $((X - \alpha)^i)_{i \in \mathbb{N}}$  est une base de  $\mathbb{K}[X]$ , car la matrice de cette famille dans la base canonique  $(X^i)_{i \in \mathbb{N}}$  est triangulaire supérieure, avec des 1 sur la diagonale. Un polynôme  $P$  de  $\mathbb{K}[X]$  peut donc s'écrire, de façon unique :

$$P = \sum_{i \in \mathbb{N}} \lambda_i (X - \alpha)^i .$$

Soit  $j = \min \{i \in \mathbb{N} \mid \lambda_i \neq 0\}$ , lorsque  $P \neq 0$ . Alors :

$$P = \sum_{i \geq j} \lambda_i (X - \alpha)^i \text{ et } \lambda_j \neq 0 .$$

Clairement,  $(X - \alpha)^j$  divise  $P$  et le quotient  $\sum_{i \geq j} \lambda_i (X - \alpha)^{i-j}$  ne s'annule pas en  $\alpha$  (puisque  $\lambda_j \neq 0$ ). Donc ce quotient n'est pas divisible par  $X - \alpha$ , et finalement :

$$m(\alpha) = j . \quad \diamond$$

Pour déterminer  $m(\alpha)$ , il suffit donc de déterminer les coefficients  $\lambda_i$ .

**Cas particulier :  $\alpha = 0$ .**

La valuation  $X$ -adique de  $P$  est appelée **valuation** (tout court) de  $P$ .

**Proposition 15 (formule de Taylor).**

Soient  $\mathbb{K}$  un corps de caractéristique nulle et  $P \in \mathbb{K}[X]$ . Alors :

$$P(Y + Z) = \sum_{i \in \mathbb{N}} \frac{P^{(i)}(Y)}{i!} Z^i .$$

**Preuve.** ◊ Par linéarité, il suffit de le vérifier sur les monômes  $X^k$ . Dans ce cas :

$$P^{(i)} = k(k-1)\dots(k-i+1) X^{k-i} \text{ si } k \geq i ,$$

$$P^{(i)} = 0 \text{ sinon.}$$

Donc :

$$\begin{aligned} \sum_{i \in \mathbb{N}} \frac{P^{(i)}(Y)}{i!} Z^i &= \sum_{i \leq k} \frac{k(k-1)\dots(k-i+1)}{i!} Y^{k-i} Z^i \\ &= \sum_{i=0}^k C_k^i Y^{k-i} Z^i = (Y+Z)^k = P(Y+Z) . \end{aligned} \quad \diamond$$

Il en résulte que, lorsque  $\mathbb{K}$  est de caractéristique nulle, on a :

$$P(X) = \sum_{i \in \mathbb{N}} \frac{P^{(i)}(\alpha)}{i!} (X - \alpha)^i,$$

formule obtenue en évaluant la formule précédente en  $(\alpha, X - \alpha)$ . Ainsi :

$$\lambda_i = \frac{P^{(i)}(\alpha)}{i!}.$$

**Corollaire.**  $m(\alpha) = \min \{i \mid P^{(i)}(\alpha) \neq 0\}$ .

En d'autres termes,  $m(\alpha)$  est l'unique entier  $m$  tel que :

$$P(\alpha) = \dots = P^{(m-1)}(\alpha) = 0 \ ; \ P^{(m)}(\alpha) \neq 0.$$

On remarquera que cette caractérisation montre que, si  $\alpha$  est d'ordre multiplicité  $m$  pour  $P$ ,  $\alpha$  est d'ordre de multiplicité  $m - k$  pour  $P^{(k)}$  ( $k = 0, \dots, m$ ).

Une telle caractérisation ne s'applique pas aux corps de caractéristique non nulle.

### 2.1.3 Résolution par radicaux

Dans certains cas, on peut déterminer les racines d'un polynôme à l'aide de formules explicites, qui font cependant intervenir des radicaux. On notera  $\sqrt[n]{a}$  un élément  $b$  de  $\mathbb{K}$  tel que  $b^n = a$ . Bien entendu, l'existence d'un tel élément n'est pas toujours assurée.

#### Équation de degré 2

Soit  $P = X^2 + pX + q$ . On suppose que  $\mathbb{K}$  n'est pas de caractéristique 2. On peut écrire :

$$P = \left(X + \frac{p}{2}\right)^2 + q - \frac{p^2}{4}.$$

Posons  $\Delta = p^2 - 4q$ . Soit  $\delta$ , s'il en existe, une racine carrée de  $\Delta$ . Ainsi :

$$P = \left(X + \frac{p}{2}\right)^2 - \left(\frac{\delta}{2}\right)^2 = \left(X + \frac{p+\delta}{2}\right)\left(X + \frac{p-\delta}{2}\right).$$

Autrement dit, la liste des racines de  $P$  est :

$$\frac{-p + \sqrt{\Delta}}{2}, \frac{-p - \sqrt{\Delta}}{2}.$$

#### Équation de degré 3

Soit  $P = X^3 + aX^2 + bX + c$ . Le polynôme  $P$  peut s'écrire :

$$\left(X + \frac{a}{3}\right)^3 + \left(b - \frac{a^2}{3}\right)X + c - \frac{a^3}{27},$$

lorsque  $\mathbb{K}$  n'est pas de caractéristique 3 ;  $P\left(X - \frac{a}{3}\right)$  s'écrit donc :

$$X^3 + \left(b - \frac{a^2}{3}\right)X - \frac{ab}{3} + \frac{2a^3}{27} + c.$$

Quitte à effectuer une translation sur la variable, on peut donc supposer que :

$$P = X^3 + pX + q.$$

Cherchons les racines de  $P$  sous la forme :

$$x = u + v.$$

Alors :  $0 = x^3 + px + q = u^3 + v^3 + (u+v)(p+3uv) + q$ .

Imposons  $uv = -\frac{p}{3}$  ;  $u$  et  $v$  doivent satisfaire :

$$u^3 + v^3 = -q.$$

Réciproquement, si  $uv = -\frac{p}{3}$  et  $u^3 + v^3 = -q$ , alors  $u + v$  est racine de  $P$ .

Nécessairement :

$$\begin{cases} u^3 + v^3 = -q \\ u^3 v^3 = -\frac{p^3}{27} \end{cases},$$

donc  $u^3$  et  $v^3$  sont racines de  $Y^2 + qY - \frac{p^3}{27}$ .

D'après l'étude de l'équation de degré 2 :

$$u^3 \in \left\{ \frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2}, \frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{2} \right\}$$

(on a supposé ici  $\mathbb{K}$  de caractéristique différente de 2).

Il y a donc éventuellement 6 valeurs de  $u$  qui répondent à cette dernière condition,  $v$  étant alors nécessairement égal à  $-\frac{p}{3u}$  (pour  $u \neq 0$ ).

Le choix des valeurs de  $u$  qui donnent effectivement lieu à une racine de  $P$  est plus délicat. Nous nous contenterons de ces remarques.

Les formules ainsi obtenues sont appelées **formules de Cardan**.

## 2.2 Cas des polynômes à coefficients réels

### 2.2.1 Polynômes irréductibles de $\mathbb{R}[X]$

Soit  $P \in \mathbb{R}[X] - \{0\}$ . On peut considérer sa décomposition en facteurs irréductibles dans  $\mathbb{C}$  :

$$P = \lambda \prod_{\alpha \in \mathbb{C}} (X - \alpha)^{m(\alpha)} \text{ où } \lambda \in \mathbb{R} - \{0\}.$$

Notons  $\bar{P}$  le polynôme **conjugué** de  $P$ , c'est-à-dire celui qui est obtenu à partir de  $P$  en conjuguant ses coefficients. Alors :

$$P = \bar{P} = \lambda \prod_{\alpha \in \mathbb{C}} (X - \bar{\alpha})^{m(\alpha)}$$

Il résulte immédiatement de l'unicité de la décomposition d'un polynôme en facteurs irréductibles que  $m(\alpha) = m(\bar{\alpha})$ . Cette égalité ne nous apporte rien si  $\alpha \in \mathbb{R}$ . En revanche, si  $\alpha \in \mathbb{C} - \mathbb{R}$ , on constate que les ordres de multiplicité de  $\alpha$  et  $\bar{\alpha}$  sont égaux. On peut ainsi, en regroupant les racines non réelles, écrire :

$$P = \lambda \prod_{\alpha \in \mathbb{R}} (X - \alpha) \prod_{\alpha \in \mathbb{C} - \mathbb{R}} (X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha})^{m(\alpha)}.$$

Les polynômes  $X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha}$  sont dans  $\mathbb{R}[X]$ .

Il résulte de cela que les polynômes irréductibles de  $\mathbb{R}[X]$  sont, ou bien les polynômes de degré 1, ou bien les polynômes de degré 2 sans racine réelle.

On peut compléter cette étude en remarquant que le polynôme  $X^2 + pX + q$  a une racine réelle si, et seulement si,  $p^2 - 4q \geq 0$  (cela résulte de l'étude de l'équation de degré 2, paragraphe 2.1.3). Les polynômes irréductibles de  $\mathbb{R}[X]$  qui ne sont pas de degré 1 sont donc ceux de la forme  $X^2 + pX + q$ , avec  $p^2 - 4q < 0$ .

**Exemple :**  $P = X^4 + 1$  n'est pas irréductible dans  $\mathbb{R}[X]$ . Pour le décomposer en facteurs irréductibles, on peut procéder comme précédemment. Les racines complexes de  $P$  sont :

$$e^{i\pi/4}, e^{-i\pi/4}, e^{3i\pi/4}, e^{-3i\pi/4}.$$

$$\begin{aligned} \text{Donc : } X^4 + 1 &= \left(X^2 - 2\cos\frac{\pi}{4}X + 1\right)\left(X^2 - 2\cos\frac{3\pi}{4}X + 1\right) \\ &= (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1) \end{aligned}$$

On peut aussi procéder directement :

$$X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1),$$

et remarquer que  $X^2 - \sqrt{2}X + 1$  et  $X^2 + \sqrt{2}X + 1$  sont irréductibles, car ils n'ont pas de racine réelle ( $X^4 + 1$  n'en a déjà pas).

Bien entendu, il n'est pas possible en général de mener de tels calculs explicitement, puisque les racines complexes d'un polynôme quelconque ne peuvent être exprimées exactement.

### 2.2.2 Racines de polynômes à coefficients réels

Les outils de l'analyse réelle permettent d'étudier les racines réelles d'un élément de  $\mathbb{R}[X]$ . Citons les plus élémentaires.

**Proposition 16.**

Soit  $P \in \mathbb{R}[X] - \{0\}$ .

① Soient  $a$  et  $b$  tels que  $a < b$  et  $P(a)P(b) \neq 0$ , et :

$$k = \sum_{a < \alpha < b} m(\alpha).$$

Alors  $(-1)^k$  et  $P(a)P(b)$  ont même signe.

② Soient  $a$  et  $b$  tels que  $a < b$  et  $P(a)P(b) < 0$ ;  $P$  admet une racine dans  $]a, b[$ .

③ Si  $P$  est de degré impair, il admet au moins une racine réelle.

**Preuve.** ◊

① Notons  $A = \{\alpha \in ]a, b[ \mid P(\alpha) = 0\}$ . Grâce à la décomposition en facteurs irréductibles dans  $\mathbb{R}[X]$ , on peut écrire :

$$P = \prod_{\alpha \in A} (X - \alpha)^{m(\alpha)} Q,$$

où  $Q$  est de signe constant dans  $]a, b[$ . Alors :

$$P(a)P(b) = \prod_{\alpha \in A} [(a - \alpha)(b - \alpha)]^{m(\alpha)} Q(a)Q(b)$$

Le signe de  $P(a)P(b)$  est égal à celui de  $\prod_{\alpha \in A} [(a - \alpha)(b - \alpha)]^{m(\alpha)}$ ,

c'est-à-dire  $(-1)^{\sum_{\alpha \in A} m(\alpha)}$ .

② Si  $P(a)P(b) < 0$ ,  $k$  est impair, donc non nul.

③ Si  $P$  est de degré impair, il ne peut être un produit de polynômes de degré 2. L'un au moins des facteurs irréductibles dans la décomposition de  $P$  est de degré 1. ◊

Notons aussi l'utilisation du théorème de Rolle.

**Proposition 17.**

Soit  $P \in \mathbb{R}[X] - \{0\}$ .

① Entre deux racines de  $P$ , il existe une racine de  $P'$ .

② Si  $P$  est scindé dans  $\mathbb{R}[X]$ , alors  $P'$  est scindé dans  $\mathbb{R}[X]$ .

**Preuve.** ◊

① C'est une application du théorème de Rolle.

② Soit  $P = \lambda \prod_{i=1}^k (X - \alpha_i)^{m(\alpha_i)}$ , avec  $\alpha_1 < \alpha_2 < \dots < \alpha_k$ , et  $m(\alpha_i) \geq 1$ , pour tout  $i \in [1, k]$ .

Alors  $P'$  est divisible par  $\prod_{i=1}^k (X - \alpha_i)^{m(\alpha_i)-1}$ , d'après le paragraphe 2.1.2.

De plus, il existe  $\beta_i \in ]\alpha_i, \alpha_{i+1}[$  (pour  $i = 1, \dots, k-1$ ) tel que  $P'(\beta_i) = 0$ . Donc  $P'$  est divisible par  $\prod_{i=1}^k (X - \alpha_i)^{m(\alpha_i)-1} \prod_{i=1}^{k-1} (X - \beta_i)$  et, compte tenu des degrés, est associé à ce dernier polynôme. ◊

## 2.3 Factorisation dans $\mathbb{Q}[X]$

### 2.3.1 Racines rationnelles d'un élément de $\mathbb{Q}[X]$

**Proposition 18.**

Soit  $P \in \mathbb{Z}[X]$ . On pose :

$$P = \sum_{i=0}^d p_i X^i, \text{ où } d = \deg P$$

Si  $\alpha = \frac{a}{b}$  est racine de  $P$ ,  $a$  et  $b$  étant deux entiers tels que  $\text{pgcd}(a, b) = 1$ , alors :

$$a \mid p_0 \text{ et } b \mid p_d.$$

**Preuve.** ◊ On écrit :

$$P\left(\frac{a}{b}\right) = \sum_{i=0}^d p_i \frac{a^i}{b^i} = 0,$$

donc  $\sum_{i=0}^d p_i a^i b^{d-i} = 0$ . En particulier,  $a$  divise  $p_0 b^d$  et, étant premier avec  $b$ , divise  $p_0$ . De même,  $b$  divise  $p_d$ . ◊

La recherche des racines rationnelles d'un élément de  $\mathbb{Q}[X]$  est donc résolue par une simple recherche de diviseurs, puisqu'un tel polynôme peut s'écrire  $\lambda P$ , où  $\lambda \in \mathbb{Q}$  et  $P \in \mathbb{Z}[X]$ .

**Exemple :** Soit  $Q = X^5 - \frac{5}{2}X^4 + 2X^3 - \frac{3}{2}X^2 - \frac{3}{2}X + 1$ .

On cherche ses racines rationnelles, soit encore celles de  $2X^5 - 5X^4 + 4X^3 - 3X^2 - 3X + 2$ . Une telle racine, de la forme  $\frac{a}{b}$ , est nécessairement telle que :

$$a \mid 2; \quad b \mid 2.$$

On peut supposer  $b > 0$ . Donc  $b = 1$  ou  $2$ , puis  $\frac{a}{b} \in \left\{-1, -\frac{1}{2}, -2, 2, \frac{1}{2}, 1\right\}$ . On vérifie alors que  $\frac{1}{2}$  et  $2$  seuls conviennent.

Après une division euclidienne, on obtient finalement :

$$Q = (X-2)\left(X-\frac{1}{2}\right)(X^3+X+1),$$

où  $X^3+X+1$  n'a pas de racine rationnelle.

Il en résulte que  $X^3+X+1$  est irréductible dans  $\mathbb{Q}[X]$ , puisque, s'il existe un diviseur  $D$  de  $X^3+X+1$  non associé à  $X^3+X+1$  et non inversible, il est de degré 1 ou 2. Par conséquent, l'un des polynômes

$D$  et  $\frac{X^3+X+1}{D}$  est de degré 1, ce qui entraîne que  $X^3+X+1$  admet une racine rationnelle.

On a ainsi obtenu la décomposition de  $Q$  en facteurs irréductibles dans  $\mathbb{Q}[X]$ .

**Corollaire.** Soit  $P \in \mathbb{Z}[X]$ , unitaire. Une racine rationnelle de  $P$  est nécessairement entière.

**Preuve.**  $\diamond$  Avec les notations de la proposition 18,  $b$  divise 1. Donc

$$\frac{a}{b} \in \mathbb{Z}. \quad \diamond$$

### 2.3.2 Critères d'irréductibilité dans $\mathbb{Q}[X]$

Une idée très élémentaire pour étudier l'irréductibilité d'un polynôme de  $\mathbb{Q}[X]$  consiste à réduire un polynôme convenable modulo un nombre premier  $p$  bien choisi. On utilisera alors le fait que,  $p$  étant premier,  $\mathbb{Z}/p\mathbb{Z}$  est un corps. On se ramène tout d'abord à un polynôme à coefficients entiers en multipliant le polynôme donné par un dénominateur commun. On supposera donc dans la suite que  $Q \in \mathbb{Z}[X]$ , et que  $c(Q) = 1$ , ce qui n'est pas restrictif.

D'après la proposition 10, on sait que  $Q$  est irréductible dans  $\mathbb{Q}[X]$  si, et seulement si, il est irréductible dans  $\mathbb{Z}[X]$ .

**Proposition 19.**

Soient  $Q \in \mathbb{Z}[X]$ , primitif, et  $p$  un nombre premier ne divisant pas le coefficient dominant de  $Q$ . Si  $\bar{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$  est irréductible, alors  $Q$  est irréductible dans  $\mathbb{Z}[X]$ .

**Preuve.**  $\diamond$   $\bar{Q}$  désigne  $\sum_{i=0}^d \bar{q}_i X^i$  lorsque  $Q = \sum_{i=0}^d q_i X^i$  (avec  $d = \deg Q$ ).

Supposons  $Q = Q_1 Q_2$ , avec  $\deg Q_1 \geq 1$  et  $\deg Q_2 \geq 1$ . Alors :

$$\bar{Q} = \bar{Q}_1 \bar{Q}_2.$$

Mais  $\deg \bar{Q} = \deg \bar{Q}_1 + \deg \bar{Q}_2$  et  $\deg \bar{Q} = \deg Q$  puisque  $\bar{q}_d \neq 0$ .

Donc, comme  $\deg \bar{Q}_1 \leq \deg Q_1$  et  $\deg \bar{Q}_2 \leq \deg Q_2$ , on a :

$$\deg \bar{Q}_1 = \deg Q_1 \geq 1 \text{ et } \deg \bar{Q}_2 = \deg Q_2 \geq 1.$$

Donc  $\bar{Q}$  est réductible dans  $\mathbb{Z}/p\mathbb{Z}[X]$ , ce qui est contraire à l'hypothèse.  $\diamond$

La mise en œuvre de ce test nécessite l'étude des polynômes irréductibles de  $\mathbb{Z}/p\mathbb{Z}[X]$ .

**Proposition 20 (critère d'Eisenstein).**

Soient  $Q \in \mathbb{Z}[X]$ , primitif et  $p$  un nombre premier divisant tous les coefficients de  $Q$  sauf le coefficient dominant, tel que  $p^2$  ne divise pas le terme constant. Le polynôme  $Q$  est alors irréductible dans  $\mathbb{Z}[X]$ .

**Preuve.**  $\diamond$  Posons  $Q = \sum_{i=0}^d q_i X^i$ .

Supposons que  $Q = Q_1 Q_2$

avec  $Q_1 = \alpha X^{d_1} + \dots + \alpha'$ ,  $d_1 \geq 1$  et  $Q_2 = \beta X^{d_2} + \dots + \beta'$ ,  $d_2 \geq 1$ .

Dans  $\mathbb{Z}/p\mathbb{Z}[X]$ , il vient :

$$\bar{Q} = \bar{Q}_1 \bar{Q}_2.$$

Or  $\bar{Q} = \sum_{i=0}^d \bar{q}_i X^i = \bar{q}_d X^d$  et  $\bar{q}_d \neq 0$ , sinon  $p$  divise tous les  $q_i$ ,

donc  $c(Q)$ . Il en résulte que  $\bar{Q}_1$  et  $\bar{Q}_2$  divisent  $X^d$ , donc sont de la forme  $\bar{\alpha} X^{d_1}$  et  $\bar{\beta} X^{d_2}$ .

Par conséquent  $p \mid \alpha'$  et  $p \mid \beta'$ , donc  $p^2 \mid \alpha'\beta'$ . Or  $\alpha'\beta'$  est le terme constant de  $Q$ . C'est une contradiction.  $\diamond$

**Exemple :**  $X^5 + 2X + 2$  est irréductible dans  $\mathbb{Z}[X]$  (donc dans  $\mathbb{Q}[X]$ ), car le nombre premier  $p = 2$  satisfait aux conditions de la proposition 20.

---

## Polynôme irréductible

§ 2.2

Rolle

§ 2.2.1

Irréductibilité

§ 2.3.2

Eisenstein

§ 2.3.2