ANNEAUX DE POLYNÔMES

Chapitre 7

Ce polycopié est très largement inspiré du polycopié utilisé par mon prédécesseur K. Koufany, que je remercie pour son travail de rédaction.

Table des matières

1. Polynômes à coefficients dans un anneau

Définition 1.1. — *Soit A un anneau commutatif unitaire. On appelle polynôme à coefficients dans A, toute suite $\mathbf{a} = (a_n)_{n\in\mathbb{N}}$ d'éléments de A, dont tous les termes sont nuls, sauf un nombre fini d'entre eux. On note $A[X]$ l'ensemble des polynômes à coefficients dans l'anneau commutatif A.*

Les éléments a_i, non nuls de cette suite sont appelés *coefficients* du polynôme $\mathbf{a}$. On définit la somme de deux polynômes $\mathbf{a} = (a_0, a_1, \ldots)$ et $\mathbf{b} = (b_0, b_1, \ldots)$ de $A[X]$ comme étant la somme des suites au sens habituel, soit

$$\mathbf{a} + \mathbf{b} = (a_0, +b_0, a_1 + b_1, \ldots).$$

Le produit $\mathbf{ab}$ est le polynôme $\mathbf{c} = (c_0, c_1, \ldots)$ où pour tout $k \in \mathbb{N}$ on pose

$$c_k = \sum_{j=0}^{k} a_j b_{k-j} = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0.$$

Posons $X = (0, 1, 0, 0, \ldots) \in A[X]$, c'est un polynôme de degré 1. Alors les polynômes $\mathbf{1}$ et X engendrent $A[X]$: on vérifie assez facilement que $X^2 = (0, 0, 1, 0 \ldots)$ et par récurrence que $X^k = (0, \ldots, 0, 1, 0, \ldots)$, où 1 est le coefficient au degré k.

L'application $j : \alpha \mapsto (\alpha, 0, 0, \ldots)$ de A dans $A[X]$ est un homomorphisme d'anneaux injectif. Elle permet donc d'identifier A avec le sous-anneau de $A[X]$ constitué des polynômes constants (de la forme $(\alpha, 0, 0, \ldots)$ où $\alpha \in A$).

En identifiant à l'aide de l'homomorphisme j tout $\alpha \in A$ avec le polynôme $(\alpha, 0 \ldots)$, tout polynôme $\mathbf{a} = (a_0, a_1, \ldots, a_n, 0, \ldots)$ de degré n, est égal à $a_0 + a_1 X + \ldots + a_n X^n$, en effet,

$$(0, \ldots, 0, a_k, 0, \ldots) = (a_k, 0, \ldots)(0, \ldots, 0, 1, 0, \ldots) = a_k X^k.$$

On vérifie assez facilement que l'ensemble $A[X]$ muni de l'addition et de la multiplication définies ci-dessus est un anneau commutatif unitaire, appelé *anneau des polynômes à une seule indéterminée à coefficients dans l'anneau* A. Le zéro de $A[X]$ est $\mathbf{0} = (0, 0, \ldots)$ et son unité est $\mathbf{1} = (1, 0, 0, \ldots)$.

Le plus grand indice n tel que $a_n \neq 0$ est appelé *degré* du polynôme $\mathbf{a}$, nous le noterons $\deg(\mathbf{a})$, dans ce cas ce coefficient a_n est appelé *coefficient dominant* di polynôme $\mathbf{a}$.

Si le coefficient dominant du polynôme a est égal à 1, ont dit que $\mathbf{a}$ est un polynôme *unitaire*.

Si $\mathbf{a} = 0$ est le polynôme nul, soit $a_k = 0$ pour tout $k \in \mathbb{N}$, on convient que $\deg(\mathbf{a}) = -\infty$.

On a donc

$$\deg(\mathbf{a} + \mathbf{b}) \leq \max(\deg(\mathbf{a}), \deg(\mathbf{b})) \text{ et } \deg(\mathbf{ab}) \leq \deg(\mathbf{a}) + \deg(\mathbf{b}).$$

Proposition 1.2. — *Supposons que l'anneau A est intègre, alors*

1. *$A[X]$ est un anneau intègre.*
2. *Pour tout $\mathbf{a}, \mathbf{b} \in A[X]$, $\deg(\mathbf{ab}) = \deg(\mathbf{a}) + \deg(\mathbf{b})$.*
3. *$(A[X])^\times = A^\times$, i.e., les unités de $A[X]$ sont les polynômes constants dont la valeur a_0 est une unité de A.*

Démonstration. — Si $\mathbf{a} = \mathbf{0}$ ou $\mathbf{b} = \mathbf{0}$ alors la propriété 2. est évidente. Supposons que $\mathbf{a} = a_0 + a_1X + \ldots + a_pX^p$ et $\mathbf{b} = b_0 + b_1X + \ldots + b_qX^p$ soient deux polynômes non nuls, avec $\deg(\mathbf{a}) = p$ et $\deg(\mathbf{b}) = q$. Le coefficient c_k de $\mathbf{ab}$ est nul pour tout $k > p + q$ et $c_{p+q} = a_pb_q$. Par conséquent, si A est intègre, $c_{p+q} = a_pb_q \neq 0$ et donc $\deg(ab) = \deg(a) + \deg(b)$. Cette propriété montre en particulier que l'anneau $A[X]$ est intègre. D'où 1. et 2.
Montrons 3. Si $\mathbf{ab} = \mathbf{1}$, alors $p+q = \deg(\mathbf{a})+\deg(\mathbf{b}) = \deg(\mathbf{ab}) = \deg(\mathbf{1}) = 0$, soit $p = 0$ et $q = 0$ et $\mathbf{a}$ et $\mathbf{b}$ sont donc deux polynômes constants $\mathbf{a} = a_0 \in A$ et $\mathbf{b} = b_0 \in A$, la condition $\mathbf{ab} = \mathbf{1}$ montre alors que $a_0b_0 = 1$ et par suite $a_0 \in A^\times$ et $b_0 \in A^\times$. On en déduit que $(A[X])^\times \subset A^\times$. L'inclusion réciproque étant évidente, on a $(A[X])^\times = A^\times$. □

Remarquons, que si $A[X]$ est intègre, alors A est lui aussi intègre, puisque A peut être considéré comme un sous-anneau de $A[X]$.

Proposition 1.3. — *Soient A, B deux anneaux commutatifs et unitaires et $\varphi : A \to B$ un morphisme d'anneaux tel que $\varphi(1_A) = 1_B$. Alors l'application $\Phi : A[X] \to B[X]$ qui à chaque polynôme $\mathbf{a} = a_0 + \ldots a_nX^n \in A[X]$ on associe $\Phi(\mathbf{a}) = \varphi(a_0) + \ldots + \varphi(a_n)X^n \in B[X]$ est un morphisme d'anneaux. De plus*

$$\mathbf{a} = \sum_{k=0}^{n} a_kX^k \in \mathrm{Ker}(\Phi) \Longleftrightarrow \forall k,\ a_k \in \mathrm{Ker}(\varphi).$$

Démonstration. — La démonstration est élémentaire. □

Soit $n \in \mathbb{N}^*$ et considérons le morphisme d'anneaux $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ tel que $\varphi(k) = \bar{k}$, classe de $k \in \mathbb{Z}$ modulo n. Alors $\Phi : \mathbb{Z}[X] \to \mathbb{Z}/n\mathbb{Z}[X]$ est donné par $\Phi(\sum a_kX^k) = \sum \bar{a}_kX^k$. Le polynôme $\bar{\mathbf{a}} = \sum \bar{a}_kX^k$ est appelé *réduction modulo n* du polynôme $\mathbf{a} = \sum a_kX^k$. Par conséquent la réduction modulo n d'une somme (respectivement produit) de polynômes de $\mathbb{Z}[X]$ est la somme (respectivement produit) des réductions de ces polynômes.

2. Division euclidienne

Théorème 2.1. — *Soient A un anneau commutatif unitaire, $\mathbf{a}$ et $\mathbf{b} = b_0 + \ldots + b_mX^m$ deux polynômes de $A[X]$ tels que le coefficient dominant b_m de $\mathbf{b}$ soit inversible dans A. Alors il existe $\mathbf{q}, \mathbf{r} \in A[X]$ uniques tels que*

$$\mathbf{a} = \mathbf{bq} + \mathbf{r} \quad \textit{avec} \quad \deg(\mathbf{r}) < \deg(\mathbf{b}).$$

De plus on a $\deg(\mathbf{q}) = \deg(\mathbf{a}) - \deg(\mathbf{b})$.
En particulier, si $A = K$ est un corps commutatif, et si $\mathbf{a} \in K[X]$, $\mathbf{b} \in K[X] - \{0\}$, alors il existe $\mathbf{q}, \mathbf{r} \in K[X]$ uniques tels que

$$\mathbf{a} = \mathbf{bq} + \mathbf{r} \quad \textit{avec} \quad \deg(\mathbf{r}) < \deg(\mathbf{b}).$$

Démonstration. — Montrons l'existence de $\mathbf{q}$ et $\mathbf{r}$ par récurrence sur le degré n de $\mathbf{a}$.
Supposons que $\mathbf{a}$ est un polynôme constant (éventuellement nul), c-à-d., $n = \deg(\mathbf{a}) = 0$ ou $\deg(\mathbf{a}) = -\infty$:

- si $\deg(b) > 0$, alors $\mathbf{q} = 0$ et $\mathbf{r} = \mathbf{a}$ convient
- si $\deg(\mathbf{b}) = 0$, alors $\mathbf{b} = b_0 \in A_*$, d'où $\mathbf{q} = (b_0^{-1}a_0)$ et $\mathbf{r} = 0$ convient.

Soit $n \in \mathbb{N}^*$ et supposons établie l'existence de $\mathbf{q}, \mathbf{r}$ pour tout polynôme $\mathbf{a} = a_0 + \ldots + a_n X^n$ de degré $\deg(\mathbf{a}) \geq n$. Considérons alors $\mathbf{a} = a_n X^n + \ldots + a_0$ un polynôme de degré n. Si $\deg(\mathbf{a}) < \deg(\mathbf{b})$, alors on peut prendre $\mathbf{q} = 0$ et $\mathbf{r} = \mathbf{a}$. Si $n = \deg(\mathbf{a}) \geq \deg(\mathbf{b}) = m$, on considère le polynôme $\mathbf{a}' = \mathbf{a} - (a_n b_m^{-1} X^{n-m})\mathbf{b}$. Donc $\deg(\mathbf{a}') \leq \max(\deg(\mathbf{a}), \deg(X^{n-m}\mathbf{b})) \leq n$, et le monôme de degré n de $\mathbf{a}'$ s'annule, d'où $\deg(\mathbf{a}') \leq n-1$. D'après l'hypothèse de récurrence, il existe $\mathbf{q}', \mathbf{r}'$ deux polynômes de $A[X]$ tels que $\mathbf{a}' = \mathbf{q}'\mathbf{b} + \mathbf{r}'$ avec $\deg(\mathbf{r}') < \deg(\mathbf{b})$ et $\deg(\mathbf{q}') = \deg(\mathbf{a}') - \deg(\mathbf{b}) \leq n - 1 - m$. Par conséquent, $\mathbf{q} = a_n b_m^{-1} X^{n-m} + \mathbf{q}'$ et $\mathbf{r} = \mathbf{r}'$ sont des polynômes à coefficients dans A vérifiant $\mathbf{a} = \mathbf{bq} + \mathbf{r}$, $\deg(\mathbf{r}) < \deg(\mathbf{b})$ et $\deg(\mathbf{q}) = n - m = \deg(\mathbf{a}) - \deg(\mathbf{b})$.

Montrons maintenant l'unicité de $\mathbf{q}$ et $\mathbf{r}$. Supposons qu'il existe $\mathbf{q}', \mathbf{r}' \in A[X]$ tels que $\mathbf{a} = \mathbf{bq}' + \mathbf{r}'$ et $\deg(\mathbf{r}') < \deg(\mathbf{b})$ On a alors $\mathbf{b}(\mathbf{q} - \mathbf{q}') = \mathbf{r}' - \mathbf{r}$. Supposons $\mathbf{q} - \mathbf{q}' \neq 0$ de degré k et soit q_k sont coefficient dominant. Comme b_m est inversible, $b_m q_k \neq 0$, d'où $\deg(\mathbf{b}(\mathbf{q} - \mathbf{q}'))\|eq \deg(\mathbf{b})$, ce qui contredit $\deg(\mathbf{r}' - \mathbf{r}) \leq \max(\deg(\mathbf{r}), \deg(\mathbf{r}')) < \deg(\mathbf{b})$. Par conséquent, $\mathbf{q}' = \mathbf{q}$ et par suite $\mathbf{r}' = \mathbf{r}$. □

Remarque 2.2. — Attention ! cela ne veut pas dire que l'anneau $A[X]$ est euclidien, car on ne peut pas effectuer la division euclidienne de n'importe quel élément de $A[X]$ par un élément non nul de $A[X]$.

Par exemple, nous avons déjà vu que l'anneau $\mathbb{Z}[X]$ n'est pas principal, donc pas euclidien. Pourtant nous pouvons faire la division de deux polynômes de $\mathbb{Z}[X]$ en considérant que ces polynômes sont à fortiori dans $\mathbb{R}[X]$ qui est euclidien. Il faut s'assurer ensuite que le quotient et le reste que nous obtenons restent à coefficients dans $\mathbb{Z}$.

Exemple 2.3. — (1) La division euclidienne de $\mathbf{a}(X) = X^7 + X^6 + X^5 + X^4 + X^3 + X^2 - 1$ par $\mathbf{b}(X) = X^5 - X^2 + 1$ dans $\mathbb{Z}[X]$ donne $\mathbf{a} = \mathbf{bq} + \mathbf{r}$ avec $\mathbf{q}(X) = X^2 - X + 1$ et $\mathbf{r}(X) = 2X^4 + 2X^3 + X^2 - X - 2$.

En passant à réduction modulo 2, c-à-d en considérant des polynômes à coefficients dans $\mathbb{Z}_2[X]$, on a $\bar{\mathbf{a}} = \bar{\mathbf{b}}\bar{\mathbf{q}} + \bar{\mathbf{r}}$, avec $\bar{\mathbf{a}}(X) = X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + \bar{1}$, $\bar{\mathbf{b}}(X) = X^5 - X^2 + \bar{1}$, $\bar{\mathbf{q}}(X) = X^2 - X + \bar{1} = X^2 + X + \bar{1}$ et $\bar{\mathbf{r}}(X) = \bar{2}X^4 + \bar{2}X^3 + X^2 - X - \bar{2} = X^2 + X$. Comme $\deg(\bar{\mathbf{r}}) = 2 < \deg(\bar{\mathbf{b}}) = 5$, alors $\bar{\mathbf{a}} = \bar{\mathbf{b}}\bar{\mathbf{q}} + \bar{\mathbf{r}}$ est bien une division euclidienne de $\bar{\mathbf{a}}$ par $\bar{\mathbf{b}}$ dans $\mathbb{Z}_2[X]$.

(2) Effectuons la division euclidienne de $\bar{\mathbf{a}}(X) = \bar{5}X^3 + X + \bar{8}$ par $\bar{\mathbf{b}}(X) = \bar{8}X^2 + \bar{4}X + \bar{1}$ dans $\mathbb{Z}_{15}[X]$. Comme $\bar{8}$ est inversible dans $\mathbb{Z}_{15}[X]$ (car $8 \wedge 15 = 1$) et que $\bar{2} \times \bar{8} = \bar{16} = \bar{1}$, on a $\bar{8}^{-1} = \bar{2}$, donc

$$\begin{array}{rrr|l}
\bar{5}X^3 & +X & +\bar{8} & \bar{8}X^2 + \bar{4}X + \bar{1} \\
\cline{4-4}
\bar{5}X^3 + \bar{10}X^2 + \bar{10}X & & & \bar{2} \times \bar{5}\,X + \bar{2} \times \bar{5} \\
\cline{1-3}
-\bar{10}X^2 & -\bar{9}X & +\bar{8} & \\
= \quad \bar{5}X^2 & +\bar{6}X & +\bar{8} & \\
\bar{5}X^2 & +\bar{10}X & +\bar{10} & \\
\cline{1-3}
 & -\bar{4}X & -\bar{2} & \\
= & \bar{11}X & +\bar{13} &
\end{array}$$

donc $\bar{\mathbf{q}}(X) = (\bar{2} \times \bar{5})X + (\bar{2} \times \bar{5}) = \bar{10}X + \bar{10}$ et $\bar{\mathbf{r}}(X) = \bar{11}X + \bar{13}$. Notez bien que $\deg(\bar{\mathbf{r}}) = 1 < \deg(\bar{\mathbf{b}}) = 2$.

3. Fonctions polynomiales

Soit A un anneau commutatif et unitaire. Soit $\mathbf{a} = a_0 + a_1X + \ldots + a_nX^n$ un polynôme à coefficients dans A. On définit l'application

$$\widetilde{\mathbf{a}} : \lambda \mapsto a_0 1 + a_1\lambda + \ldots + a_n\lambda^n$$

de A dans A appelée *fonction polynomiale* associée à $\mathbf{a}$.

Si $\mathbf{a} = a_0 + a_1X + \ldots + a_nX^n$ et $\mathbf{b} = b_0 + b_1X + \ldots + b_mX^m$ sont deux polynômes de $A[X]$, alors il est clair que pour tout $\lambda \in A$,

$$\widetilde{(\mathbf{a} + \mathbf{b})}(\lambda) = \widetilde{\mathbf{a}}(\lambda) + \widetilde{\mathbf{b}}(\lambda),\ \widetilde{(\mathbf{ab})}(\lambda) = \widetilde{\mathbf{a}}(\lambda)\widetilde{\mathbf{b}}(\lambda),\ \widetilde{\mathbf{1}}(\lambda) = 1$$

On en déduit que l'application $\varphi : \mathbf{a} \mapsto \widetilde{\mathbf{a}}$ est un morphisme d'anneaux de $A[X]$ dans l'anneau $\mathcal{F}(A, A)$ des fonctions de A dans A.

Ce morphisme n'est pas en général injectif, il faut donc faire attention à bien distinguer un polynôme $\mathbf{a}$ de sa fonction polynomiale associée $\widetilde{\mathbf{a}}$. Autrement dit, si les fonctions polynomiales associées à deux polynômes sont égales, les deux polynômes ne sont pas nécessairement égaux.

Par exemple, si nous considérons l'anneau $A = \mathbb{Z}/2\mathbb{Z}$ alors le polynôme $\mathbf{a} = X^2 - X \in \mathbb{Z}/2\mathbb{Z}[X]$ est un polynôme non nul, cependant sa fonction polynomiale associée est nulle, puisque pour tout $\bar{k} \in \mathbb{Z}/2\mathbb{Z}$, $\widetilde{\mathbf{a}}(\bar{k}) = \bar{k}^2 - \bar{k} = \bar{0}$.

Théorème 3.1 **(Théorème du reste).** — *Soit $\mathbf{a} \in A[X]$ et λ un élément de A. Alors il existe un unique polynôme $\mathbf{q} \in A[X]$ tel que*

$$\mathbf{a} = (X - \lambda)\mathbf{q} + \widetilde{\mathbf{a}}(\lambda).$$

Démonstration. — Puisque le coefficient dominant du polynôme $X-\lambda$ est égal à 1 (donc inversible dans A), alors on peut effectuer la division euclidienne de $\mathbf{a}$ par $X-\lambda$. Il existe alors $\mathbf{q}, \mathbf{r} \in A[X]$ uniques tels que $\mathbf{a} = (X-\lambda)\mathbf{q} + \mathbf{r}$ avec $\deg(\mathbf{r}) < \deg(X-\lambda) = 1$, d'où $\mathbf{r}$ est un polynôme constant, $\mathbf{r} = c \in A$, et on a $c = \widetilde{\mathbf{a}}(\lambda)$. □

Définition 3.2. — *On dira que $\lambda \in A$ est une racine (ou un zéro) du polynôme $\mathbf{a} \in A[X]$ si $\widetilde{\mathbf{a}}(\lambda) = 0$.*

On dit qu'un corps K est algébriquement clos, si tout polynôme $\mathbf{a} \in K[X]$, non constant, admet au moins une racine dans K. D'après le théorème de d'Alembert, le corps $\mathbb{C}$ est algébriquement clos.

Corollaire 3.3. — *Soit $\mathbf{a} \in A[X]$ et $\lambda \in A$. Alors λ est une racine de $\mathbf{a}$ si et seulement si $X-\lambda$ divise $\mathbf{a}$ dans $A[X]$.*

Démonstration. — Si λ est une racine de alors $\mathbf{a}$, alors d'après le théorème du reste $\mathbf{a} = (X-\lambda)\mathbf{q} + \widetilde{\mathbf{a}}(\lambda) = (X-\lambda)\mathbf{q}$, d'où $X-\lambda$ divise $\mathbf{a}$. Réciproquement, si $X-\lambda$ divise $\mathbf{a}$, alors $\mathbf{a} = (X-\lambda)\mathbf{q}$ et par suite $\widetilde{\mathbf{a}}(\lambda) = (\lambda-\lambda)\widetilde{\mathbf{q}}(\lambda) = 0$. □

Corollaire 3.4. — *Supposons que l'anneau A soit intègre. Soit $\mathbf{a} \in A[X]$ un polynôme non nul admettant k racines distinctes $\lambda_1, \ldots, \lambda_k$. Alors il existe un polynôme $\mathbf{q} \in A[X]$ (de degré $\deg(\mathbf{a}) - k$) tel que $\mathbf{a} = (X-\lambda_1)\cdots(X-\lambda_k)\mathbf{q}$. En particulier, $k \leq \deg(\mathbf{a})$.*

Démonstration. — D'après le corollaire 3.3, $\mathbf{a} = (X-\lambda_1)\mathbf{q}_1$ avec $\deg(\mathbf{q}_1) = \deg(\mathbf{a}) - 1$. D'où, $0 = \widetilde{\mathbf{a}}(\lambda_2) = (\lambda_2-\lambda_1)\widetilde{\mathbf{q}}(\lambda_2)$. Or $\lambda_1 \neq \lambda_2$ et A intègre, donc $\widetilde{\mathbf{q}}(\lambda_2) = 0$ et λ_2 est racine de $\mathbf{q}_1$. D'après le même proposition, on a aussi, $\mathbf{q}_1 = (X-\lambda_2)\mathbf{q}_2$ et donc $\mathbf{a} = (X-\lambda_1)(X-\lambda_2)\mathbf{q}_2$ avec $\deg(\mathbf{q}_2) = \deg(\mathbf{q}_1) - 1 = \deg(\mathbf{a}) - 2$. Pour obtenir le résultat on poursuit avec un raisonnement par récurrence. □

Corollaire 3.5. — *Soit K un corps algébriquement clos. Tout polynôme $\mathbf{a} = a_nX^n + \ldots + a_1X + a_0 \in K[X]$ de degré $n \geq 1$ se factorise sous la forme $\mathbf{a} = a_n(X-\lambda_1)\ldots(X-\lambda_n)$.*

Corollaire 3.6. — *Supposons A intègre, alors tout polynôme $\mathbf{a} \in A[X]$ non nul de degré n a au plus n racines distinctes dans A.*

Corollaire 3.7. — *Soit A un anneau commutatif, unitaire, intègre et infini. Alors le morphisme $\Phi : \mathbf{a} \mapsto \widetilde{\mathbf{a}}$ est injectif. Autrement dit l'égalité formelle de deux polynômes de $A[X]$ est équivalente à l'égalité des fonctions polynomiales associées.*

Démonstration. — Si $\mathbf{a} \in \mathrm{Ker}(\Phi)$, alors $\widetilde{\mathbf{a}}$ est la fonction nulle, c-à-d. $\widetilde{\mathbf{a}}(\lambda) = 0$ pour tout $\lambda \in A$. Donc le polynôme admet une infinité de racines dans A et d'après le corollaire **??** le polynôme est nul. □

4. Polynôme dérivé, formule de Taylor

Dans ce paragraphe on suppose que A est un corps commutatif, noté K.

Définition 4.1. — *Soit* $\mathbf{a} = a_0 + a_1X + \ldots + a_nX^n \in K[X]$. *On appelle polynôme dérivé de* $\mathbf{a}$ *le polynôme* $\mathbf{a}' = a_1 + 2a_2X + \ldots + na_nX^{n-1}$.
Si $\mathbf{a}$ *est un polynôme constant, son polynôme dérivé est nul.*

Il est clair que si $\mathbf{a}, \mathbf{b} \in K[X]$ et $\lambda \in K$ alors

$$(\mathbf{a}+\mathbf{b})' = \mathbf{a}' + \mathbf{b}',\ (\mathbf{ab})' = \mathbf{a}'\mathbf{b} + \mathbf{ab}',\ (\lambda\mathbf{a})' = \lambda\mathbf{a}'.$$

Soit K un corps de caractéristique nulle. Si le polynôme dérivé $\mathbf{a}'$ d'un polynôme $\mathbf{a} \in K[X]$ est nul, alors $\mathbf{a}$ est un polynôme constant. Cependant, ce résultat est faux si la caract$(K) = p \neq 0$. Par exemple, si p est nombre premier, alors le polynôme $\mathbf{a} = X^p \in \mathbb{Z}/p\mathbb{Z}[X]$ est non nul, mais $\mathbf{a}' = pX^{p-1} = 0$.

On définit par récurrence la dérivée d'ordre $k \in \mathbb{N}$, $\mathbf{a}^{(k)}$ du polynôme $\mathbf{a} \in K[X]$ de la façon suivante : $\mathbf{a}^{(0)} = \mathbf{a}$, $\mathbf{a}^{(1)} = \mathbf{a}$, et $\mathbf{a}^{(k+1)} = (\mathbf{a}^{(k)})'$ pour $k \geq 2$.
On peut aussi montrer par récurrence sur $m \in \mathbb{N}$, que

$$(\mathbf{a}^m)' = m\mathbf{a}'\mathbf{a}^{m-1}$$

et la formule de Leibniz

$$(\mathbf{ab})^{(m)} = \sum_{k=0}^{m} C_m^k \mathbf{a}^{(k)}\mathbf{b}^{(m-k)}.$$

Si $\mathbf{a} = a_0 + a_1X + \ldots + a_nX^n$, alors on obtient pour tout $k \in \mathbb{N}$, $0 \leq k \leq n$,

$$\mathbf{a}^{(k)} = k!a_k + \ldots + n(n-1)\cdots(n-k+1)a_nX^{n-k}.$$

D'où

$$\widetilde{\mathbf{a}^{(k)}}(0) = \widetilde{\mathbf{a}}^{(k)}(0) = k!a_k$$

Théorème 4.2 **(Formule de Taylor)**. — *Soit* K *un corps commutatif de caractéristique nulle et* $\mathbf{a} = a_0 + a_1X + \ldots + a_nX^n \in K[X]$ *un polynôme de degré* n. *Alors*

$$\mathbf{a}(X) = \sum_{k=0}^{n} \frac{1}{k!}\widetilde{\mathbf{a}}^{(k)}(0)X^k.$$

Démonstration. — Comme la caractéristique de K est nulle, pour tout $k \in \mathbb{N}$, $k!1 \neq 0$. L'élément $k!1$ est donc inversible, notons sont inverse par $\frac{1}{k!}$. Comme $\widetilde{\mathbf{a}}^{(k)}(0) = k!a_k = (k!1)a_k$, on a $a_k = \frac{1}{k!}\widetilde{\mathbf{a}}^{(k)}(0)$ d'où la formule de Taylor. □

Corollaire 4.3. — *Pour tout élément $\lambda \in K$,*

$$\mathbf{a}(X) = \sum_{k=0}^{n} \frac{1}{k!} \widetilde{\mathbf{a}}^{(k)}(\lambda)(X-\lambda)^k.$$

On en déduit que $(X-\lambda)^m$ divise le polynôme $\mathbf{a}$ si et seulement si

$$\widetilde{\mathbf{a}}(\lambda) = 0,\ \widetilde{\mathbf{a}}'(\lambda) = 0, \ldots, \widetilde{\mathbf{a}}^{(m-1)}(\lambda) = 0.$$

5. Théorèmes de transfert aux anneaux de polynômes

Il est naturel de se poser la question suivante : L'anneau de polynôme $A[X]$ est-il euclidien (resp. principal, factoriel) si l'anneau A est euclidien, (resp. principal, factoriel) ?

Nous savons déjà que si K est un corps alors l'anneau $K[X]$ est euclidien et donc principal.

Nous avons aussi vu que l'anneau $\mathbb{Z}[X]$ n'est pas principal et donc pas euclidien même si l'anneau $\mathbb{Z}$, lui, est euclidien et donc principal.

Il faut donc retenir :

$$A \text{ euclidien} \not\Rightarrow A[X] \text{ euclidien}$$

$$A \text{ principal} \not\Rightarrow A[X] \text{ principal}$$

Théorème 5.1. — *Soit A un anneau commutatif et unitaire. On a*

$$(i)\ A[X] \textit{ est euclidien} \Leftrightarrow (ii)\ A[X] \textit{ est principal} \Leftrightarrow (iii)\ A \textit{ est un corps}$$

Démonstration. — Nous avons déjà vu que $(iii) \Rightarrow (i) \Rightarrow (ii)$.

Supposons maintenant que $A[X]$ est principal. Considérons l'application $f : A[X] \to A$, qui associé à chaque polynôme $P = \sum a_k X^k$ le coefficient constant a_0. Il est facile de voir que f est un morphisme d'anneaux, de plus il est surjectif. Soit maintenant $P = \sum_{k=0}^{n} a_k X^k \in \operatorname{Ker} f$, on a $0 = f(P) = a_0$, d'où $P = X(a_1 + a_2 X + \cdots a_n X^{n-1})$. Il s'en suite que $\operatorname{Ker} f$ coincide avec l'idéal $\langle X \rangle$ engendré par le polynôme X. Le théorème d'isomorphisme conduit à un isomorphisme d'anneaux $A[X]/\langle X \rangle \simeq A$.

Montrons que $A[X]/\langle X \rangle$ est un corps, ce qui implique que A est un corps. Il suffit pour cela de montrer que l'idéal $\langle X \rangle$ est maximal et ceci est équivalent à montrer que $\langle X \rangle$ est premier puisque $A[X]$ est principal. De manière encore équivalente, puisque $A[X]$ est principal et donc factoriel, il suffit de montrer que X est un élément irréductible de $A[X]$.

Posons donc $P = X$ et supposons que $P = Q_1 Q_2$ avec $Q_1, Q_2 \in A[X]$. Comme $A[X]$ est intègre, $1 = \deg(P) = \deg(Q_1) + \deg(Q_2)$. Il s'ensuite que l'un des deux polynômes Q_i est de degré 1 et l'autre une constante. On peut

donc supposer que $Q_1 = a$ et $Q_2 = bX$ avec $a, b \in A$. Comme $P = Q_1Q_2$, on a $X = abX$ et $ab = 1_A$, ce qui implique que le polynôme Q_1 est inversible (et que Q_2 est associé à P). Ainsi P est irréductible dans $A[X]$ et par suite l'idéal $\langle X \rangle$ est premier. D'où $(ii) \Rightarrow (iii)$. □

6. Irréductibilité des polynômes à coefficients dans un anneau factoriel

Définition 6.1. — *Soit A un anneau factoriel. Soit P un élément de $A[X]$ tel que $P \notin A$. On appelle* **contenu** *de P, noté $c(P)$, un pgcd dans A des coefficients de P. Si $c(P) = 1$ on dit que P est* **primitif**.

Remarque 6.2. — (1) Comme pour la notion de pgcd, la notion de contenu d'un polynôme est définie à un élément inversible près : si $c(P) = a$ alors $c(P) = ua$ pour tout $u \in A^\times$.

(2) On a (P primitif) $\Leftrightarrow$ ($\deg P \geq 1$ et $c(P) = 1$) $\Leftrightarrow$ ($\deg P \geq 1$ et $c(P) \in A^\times$).

(3) Tout polynôme unitaire est primitif.

(4) Tout polynôme $P \in A[X]$ tel que $P \notin A$ s'écrit $P = c(P)P_1$ avec P_1 primitif.

Lemme 6.3. — *Soit A un anneau factoriel. Soient P_1 et P_2 deux polynômes primitifs de $A[X]$. Soient a_1, a_2 deux éléments non nuls de A. Si $a_1P_1 = a_2P_2$, alors a_1 et a_2 sont associés dans A et P_1 et P_2 sont associés dans $A[X]$.*

Démonstration. — Comme P_1 est primitif, $c(a_1P_1) = a_1$. De même $c(a_2P_2) = a_2$. Donc a_1 et a_2 sont deux pgcd des coefficients du polynôme $a_1P_1 = a_2P_2$. Ils sont donc associés dans A : il existe $u \in A^\times$ tel que $a_2 = ua_1$. On a alors $a_1P_1 = ua_1P_2$. Or comme A est intègre, $A[X]$ l'est aussi, d'où $P_1 = uP_2$. Comme u est inversible dans $A[X]$, on conclut que P_1 et P_2 sont associés. □

***Lemme 6.4* (de Gauss)**. — *Soit A un anneau factoriel. Soient P et Q deux polynômes de $A[X]$. On a :*

(1) P et Q sont primitifs si, et seulement si, PQ est primitif;

(2) $c(PQ) = c(P)c(Q)$.

Démonstration. — Supposons que P et Q soient primitifs et que PQ ne le soit pas. Comme $c(PQ)$ n'est pas inversible dans l'anneau A, il est divisible par au moins un élément p irréductible et donc premier. Considérons l'anneau intègre $B = A/pA$. La surjection canonique $\pi : A \to B$ se prolonge canoniquement en un morphisme d'anneaux $\Phi : A[X] \to B[X]$ défini par $\Phi(\sum a_iX^i) = \sum \pi(a_i)X^i$. Comme $c(P) = 1$, l'élément p ne divise pas tous les coefficients de P, donc $\Phi(P) \neq 0$. De même $\Phi(Q) \neq 0$. Comme B est intègre, $B[X]$ l'est aussi, donc $\Phi(P)\Phi(Q) \neq 0$, c'-à-d. $\Phi(PQ) \neq 0$. Or, p divise

$c(PQ)$, donc tous les coefficients de PQ de PQ, donc $\Phi(PQ) = 0$. D'où une contradiction. On a ainsi montré que P et Q primitifs implique PQ primitif.

Réciproquement, supposons PQ primitif. On peut écrire $P = c(P)P_1$ et $Q = c(Q)Q_1$ avec P_1 et Q_1 primitifs. Alors P_1Q_1 est primitif d'après ce qui précède, et l'égalité $PQ = c(P)c(Q)P_1Q_1$ montre que $c(P)c(Q)$ est associé à 1 dans A, donc inversible dans A. D'où $c(P) \in A^\times$ et $c(Q) \in A^\times$ de sorte que P et Q sont primitifs.

Soient maintenant P et Q deux éléments quelconques de $A[X]$. On pose $P = c(P)P_1$, $Q = c(Q)Q_1$ et $PQ = c(PQ)R_1$ avec P_1, Q_1 et R_1 primitifs. Comme $c(PQ)R_1 = c(P)c(Q)P_1Q_1$ et que P_1Q_1 est primitif (d'après la première partie de la démonstration), on a $c(PQ)$ est associé à $c(P)c(Q)$ dans A et donc à un élément inversible près, $c(PQ) = c(P)c(Q)$. □

Lemme 6.5. — *Soient A un anneau factoriel et K son corps de fractions. Tout polynôme $P \in K[X]$ tel que $P \notin K$ peut s'écrire $P = qP_1$ avec $q \in K^\times$ et $P_1 \in A[X]$ primitif dans $A[X]$.*

Démonstration. — Posons $P = \sum_{j=0}^{n} \frac{a_j}{s_j} X^j \in K[X]$ avec $n \geq 1$, $a_j \in A$, $s_j \in A \setminus \{0\}$ et $a_n \neq 0$. Soit s un ppcm des s_j, on peut écrire $P = \frac{1}{s} \sum_{j=0}^{n} a'_j X^j$ avec $a'_j \in A$. Soit d un pgcd des a'_j et écrivant $a'_j = db_j$, les b_j sont premiers entre eux dans A. Donc $P = \frac{d}{s} P_1$ avec $P_1 = \sum_{j=0}^{n} b_j X^j$ primitifs et $\frac{d}{s} \in K^\times$. □

Lemme 6.6. — *Soit $P \in A[X]$ primitif et soit $Q, R \in K[X]$ tels que $P = QR$. Alors il existe des éléments $q, r \in K$ tels que $P = (qQ)(rR)$ et $qQ, rR \in A[X]$.*

Démonstration. — Soit $Q, R \in K[X]$ tels que $P = QR$. En utilisant le Lemme 6.5, on écrit $qQ = Q_1$ et $rR = R_1$ avec $Q_1, R_1 \in A[X]$ primitifs. On a alors $qrP = Q_1R_1$, donc

$$qr = c(qrP) = c(Q_1R_1) = c(Q_1)c(R_1) = 1.$$

Ceci montre que $qr = 1$, dont on déduit que $P = QR = Q_1R_1$. □

Théorème 6.7. — *Soient A un anneau factoriel et K son corps de fractions. Les polynômes irréductibles de $A[X]$ sont :*

(1) les éléments de A irréductibles dans A (polynômes constants);

(2) les polynômes de $A[X]$ de degré ≥ 1, primitifs et irréductibles dans $K[X]$.

Démonstration. — Il est clair que les éléments de $A[X]$ de degré 0 sont des éléments irréductibles si et seulement si ce sont des éléments irréductibles de A. Montrons donc qu'un polynôme non constant est irréductible dans $A[X]$ si et seulement si il est primitif et irréductible dans $K[X]$.

Soit donc d'abord P tel que $\deg(P) \geq 1$ et P est irréductible dans $A[X]$. On peut écrire $P = c(P)P_1$ avec P_1 primitif, et comme P est irréductible et P_1 n'est pas inversible, on a $c(P)$ inversible, soit P primitif. Pour montrer que P est irréductible dans $K[X]$, écrivons $P = QR$ avec $Q, R \in K[X]$. Par le Lemme 6.6, soit $q, r \in K$ tels que $P = (qQ)(rR)$ et $qQ, rR \in A[X]$. L'irréductibilité de P dans $A[X]$ donne que qQ ou rR est dans $A^\times$, et donc Q ou R est une unité de $K[X]$.

Soit finalement P primitif et irréductible dans $K[X]$. Soit une écriture $P = QR$ de P comme produits d'éléments de $A[X]$. Alors Q et R sont en particulier dans $K[X]$, et comme P est irréductible dans $K[X]$, on peut par exemple supposer que $Q \in K[X]^\times = K^\times$. On écrit alors $1 = c(P) = Qc(R)$, ce qui montre que Q est inversible dans A. □

Théorème 6.8. — *Si A est un anneau factoriel, alors l'anneau $A[X]$ est factoriel.*

Démonstration. — Montrons d'abord l'existence d'une décomposition en produits de facteurs irréductibles d'un élément donné P. On écrit d'abord $P = c(P)P_1$ avec $P_1 \in A(X]$ primitif. Si P_1 est irréductible dans $K[X]$, il est donc irréductible dans $A[X]$. Sinon, par le Lemme 6.6, on peut l'écrire sous la forme Q_1R_1 avec $Q_1, R_1 \in A[X]$ de degrés positifs et primitifs. Par récurrence sur le degré, on peut écrire Q_1 et R_1 comme produits de polynômes primitifs et irréductibles dans $K[X]$: disons $P_1 = S_1 \cdots S_k$. Par factorialité de A, on peut aussi écrire $c(P)$ comme produit d'irréductibles de A : disons $c(P) = p_1 \cdots p_l$. On obtient

$$P = p_1 \cdots p_l \cdot S_1 \cdots S_k \,,$$

et par le Théorème 6.7, c'est une décomposition en produit d'irréductibles de $A[X]$.

Pour l'unicité, supposons qu'on a les décompositions

$$P = p_1 \cdots p_k S_1 \cdots S_m = q_1 \cdots q_l T_1 \cdots T_n$$

avec p_i, q_j des éléments irréductibles de A et S_i, T_j des polynômes irréductibles de $A[X]$ et de degré strictement positif. Alors $c(P) = p_1 \cdots p_k = q_1 \cdots q_l$, de sorte que $k = l$ et il existe une permutation σ telle que p_i soit associé à $q_{\sigma(i)}$. De plus, on déduit alors que $S_1 \cdots S_m = T_1 \cdots T_n$. Le polynôme S_1, irréductible dans $K[X]$ qui est euclidien, est premier. Puisque S_1 divise $S_1 \cdots S_m = T_1 \cdots T_n$, il existe donc un entier j tel que S_1 divise T_j dans $K[X]$. Etant irréductibles dans $K[X]$, S_1 et T_j sont associés dans $K[X]$, et étant primitifs tous les deux, ils sont en fait associés dans $A[X]$. □

7. Critère d'irréductibilité d'Eisenstein

Théorème 7.1. — *Soient A un anneau factoriel et K son corps de fractions. Soit $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un élément de $A[X]$ de dégré $n \geq 1$. On suppose qu'il existe dans A un élément p, premier dans A, et satisfaisant les trois conditions suivantes :*

(1) p divise $a_0, a_1, \cdots, a_{n-1}$;

(2) p ne divise par a_n;

(3) p^2 ne divise par a_0.

Alors P est irréductible dans $K[X]$.

Si de plus P est primitif dans $A[X]$ (en particulier s'il est unitaire dans $A[X]$), alors P est irréductible dans $A[X]$.

Démonstration. — □

Exemples 7.2. — (1) $P = X^7 + 4x^5 + 12X^2 + 2 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$ par application du critère d'Eisenstein avec nombre premier $p = 2$. Comme P est unitaire, il est primitif, et par suite il est irréductible dans $\mathbb{Z}[X]$.

(2) Le critère d'Eisenstein s'applique parfois après un changement de variable convenable : considérons par exemple le polynôme $P(X) = X^3 - 3X + 1$. On ne peut pas appliquer directement le critère à ce polynôme. On pose $X = Y - 1$ et on obtient $Q(Y) = P(Y-1) = (Y-1)^3 - 3(Y-1) + 1 = Y^3 - 3Y^2 + 3$ Par application du critère d'Eisenstein à ce polynôme avec le nombre premier $p = 3$, on montre que q'il est irréductible dans $\mathbb{Q}[X]$, par conséquent P est irréductible $\mathbb{Q}[X]$ et comme il est unitaire, donc primitif, il est irréductible dans $\mathbb{Z}[X]$.

Remarques 7.3. — (1) Si K est un corps alors tout polynôme $P = aX + b \in K[X]$ de degré 1 est irréductible dans $K[X]$.

(2) Si A est un anneau factoriel et si $a \wedge b = 1$, alors $P = aX + b \in A[X]$ est irréductible dans $A[X]$.

(3) Soit K un coprs. Pour qu'un polynôme $P \in K[X]$ de degré 2 ou 3 soit irréductible dans $K[X]$, il faut et il suffit qu'il n'ait pas de racines dans le corps K. En effet, si P est réductible, il est existe $Q, R \in K[X]$ tels que $q := \deg Q \geq 1$, $r := \deg R \geq 1$ et $P = QR$. On a $q + r = \deg P = 2$ ou 3. L'un des degrés q ou r est égal à 1. Par exemple, si $q = 1$, alors Q est de la forme $aX + b$ où $a \neq 0$ et P admet pour racine $-\frac{b}{a}$. Réciproquement, si P a une racine $\alpha \in K$, il existe $Q \in K[X]$ avec $\deg Q = \deg P - 1 \neq 0$, tel que $P(X) = (X - \alpha)Q(X)$ et P n'est pas irréductible.

Cette caractérisation ne s'applique plus pour $\deg P \geq 4$. Par exemple $X^4 + X^2 + 1 = (X^2 + X + 1)(X^2 - X + 1)$ n'est pas irréductible dans $\mathbb{R}[X]$ et il n'as pas de racine dans $\mathbb{R}$.

Le résultat suivant est spécifique pour l'anneau de polynômes $\mathbb{Z}[X]$.

Proposition 7.4. — *Soit $P = a_nX^n + \cdots + a_1X + a_0$ un polynôme de degré ≥ 1 de $\mathbb{Z}[X]$.*
S'il existe un nombre premier p tel que la réduction de P modulo p, $\bar{P} = \bar{a}_nX^n + \cdots + \bar{a}_1X + \bar{a}_0 \in \mathbb{Z}/p\mathbb{Z}[X]$ verifie $\bar{a}_n \neq \bar{0}$ et $\bar{P}$ irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Z}[X]$.

Démonstration. — En effet, si $P = QR$ avec $Q = b_qX^q + \cdots + b_0$, $R = c_rX^r + \cdots + c_0$ deux polynômes de degrés $q \geq 1$ et $r \geq 1$, donc modulo p on a

$$\bar{a}_nX^n + \cdots + \bar{a}_0 = (\bar{b}_qX^q + \cdots + \bar{b}_0)(\bar{c}_rX^r + \cdots + \bar{c}_0)$$

avec $\bar{b}_q \neq 0$ et $\bar{c}_r \neq 0$ car $\bar{a}_n \neq 0$ et $\mathbb{Z}/p\mathbb{Z}$ intègre. Donc $\deg \bar{Q} = \deg Q = q$ et $\deg \bar{R} = \deg R = r$. Or $\bar{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ donc, par exemple $\bar{Q}$ est inversible, c-à-d. $\deg \bar{Q} = 0$ ce qui conduit à $\deg Q = 0$ ce qui est absurde. Par conséquent P est irréductible dans $\mathbb{Z}[X]$. □