

CH5) Les polynômes et leurs racines

Dans ce texte, A désigne un anneau. On le supposera toujours *intègre*. On supposera le plus souvent que c'est un corps, auquel cas on adoptera la notation K .

Une motivation fondamentale et historique de l'algèbre en général, et l'arithmétique en particulier, est de trouver les racines des polynômes ! C'est notamment une des raisons de l'émergence du corps des nombres complexes. Cette question a des ramifications dans tous les domaines des mathématiques, notamment en analyse (par exemple, le Théorème de D'Alembert-Gauss), mais aussi en géométrie, notamment la géométrie algébrique, où il s'agit de comprendre le lieu d'annulation d'une collection de polynômes **à plusieurs indéterminées**.

1. COMPLÉMENT SUR LES RACINES

Dans toute section, on ne considère que l'anneau des polynômes $K[X]$ sur un corps.

1.1. Ordre de multiplicité

Théorème - Définition 1.1. Soit P un polynôme de $K[X]$, a un élément de K et $k \geq 1$ un entier. Les assertions suivantes sont équivalentes :

- (1) Il existe $Q \in K[X]$ tel que $P = (X - a)^k Q$ et $Q(a) \neq 0$,
- (2) $(X - a)^k$ divise P mais $(X - a)^{k+1}$ ne divise pas P .

Lorsque ces assertions sont vraies, on dit que a est une racine de P d'ordre de multiplicité k , ou encore, que k est l'ordre de multiplicité de la racine a de P .

Si $(X - a)^p$ divise P , on dit que a est une racine de P d'ordre (de multiplicité) au moins p .

Démonstration.

- (1) \Rightarrow (2) : Alors $(X - a)^k$ divise P . Soit D le quotient de la division euclidienne de Q par $X - a$: $Q = (X - a).D + Q(a)$. Donc $P = (X - a)^{k+1}.D + Q(a).(X - a)^k$. Le reste de la division euclidienne de P par $(X - a)^{k+1}$ est donc le polynôme de degré k non-nul $Q(a).(X - a)^k$, donc $(X - a)^{k+1}$ ne divise pas P .
- (2) \Rightarrow (1) : Alors $P = (X - a)^k Q$, et $X - a$ ne divise pas Q . On a déjà montré qu'alors a ne peut pas être racine de Q .

□

Comme $(X - a)^k$ est d'ordre k , toute racine de P est de multiplicité au plus $\deg P$, et il n'y a égalité que si $P = b.(X - a)^n$ avec $b \in K \setminus \{0\}$. Plus généralement :

Théorème 1.2. Soit P un polynôme de $K[X]$, a_1, \dots, a_r r éléments distincts de K et k_1, \dots, k_r des entiers non-nul. Alors, P admet chacun des a_i comme racine d'ordre au moins k_i si et seulement si il est divisible par le produit $(X - a_1)^{k_1} \dots (X - a_r)^{k_r}$.

Démonstration. Ceci découle du fait du théorème de décomposition, et du fait que comme les a_i sont distincts, les polynômes $(X - a_i)^{k_i}$ sont deux-à-deux premiers. □

En fait, le théorème de décomposition montre que l'ordre d'une racine a est précisément l'entier $\nu_P(X - a_i)$ apparaissant dans la décomposition en facteurs premiers.

Corollaire 1.3. Si $P \in K[X]$ est un polynôme non-nul admettant des racines a_1, \dots, a_r d'ordres respectifs au moins k_1, \dots, k_r , alors :

$$k_1 + \dots + k_r \leq \deg P$$

□

Théorème - Définition 1.4. Soit P un polynôme de $K[X]$. Les deux assertions suivantes sont équivalentes :

- P est constant ou admet des racines dans K dont la somme des ordres de multiplicité est $\deg P$,
- P est de la forme $a.(X - a_1)^{k_1} \dots (X - a_r)^{k_r}$ avec $a, a_i \in K$ et $k_i \in \mathbb{N}$.

Lorsque ces assertions sont vérifiées, on dit que P est un **polynôme scindé (sur K)**. □

1.2. Ordre de multiplicité et polynôme dérivé

Proposition 1.5. Soit P un polynôme de $K[X]$, a un élément de K et $k \geq 1$ un entier. Si a est une racine de P d'ordre de multiplicité $\geq k$, alors, pour tout entier i entre 0 et $k-1$ le polynôme dérivé $P^{(i)}$ d'ordre i admet a comme racine. Inversement, si a est racine de $P^{(i)}$ pour tout $0 \leq i < k$, et que K est de caractéristique nulle, a est une racine de P d'ordre de multiplicité $\geq k$.

Démonstration.

- **Si a est racine d'ordre k :** Alors $P = (X-a)^k Q$. En dérivant on obtient $P' = k(X-a)^{k-1}Q + (X-a)^k Q'$. En itérant et en utilisant la règle de Leibniz, on voit que tous les $P^{(i)}$ pour $i < k$ est une somme de termes qui ont tous une puissance non-triviale de $(X-a)$ en facteur. D'où la conclusion.
- **Si les $P^{(i)}$ pour $i < k$ s'annulent en a et que K est de caractéristique nulle :** Comme a est racine de $P = P^{(0)}$ on a $P = (X-a)Q_0$. En dérivant : $P' = Q_0 + (X-a)Q_0'$, d'où $Q_0(a) = 0$, et donc $Q_0 = (X-a)Q_1$ et $P = (X-a)^2 Q_1$. De proche en proche (par récurrence), on montre ainsi que pour tout $i < k$ on a $P = (X-a)^i Q_i$: en effet, une fois ceci établi pour i , on voit alors que la dérivée i -ième de P est une somme de termes ayant une puissance de $X-a$ en facteur, plus un terme égal à $i!Q_i$. Comme celui-ci s'annule en a , on a $Q_i = (X-a)Q_{i+1}$ ce qui établit la validité de la récurrence. □

Exercice 1. Soit P le polynôme $X^3 + X$ de $\mathbb{Z}/2\mathbb{Z}$. Montrer que 1 est racine de toutes les dérivées de P , mais que 1 n'est qu'une racine double de P .

Exercice 2. Montrer que pour tout corps K , $a \in K$ est une racine d'un polynôme P de $K[X]$ d'ordre ≥ 2 si et seulement si a est racine de P et P' .

1.3. Corps algébriquement clos

Définition 1.6. Le corps K est dit **algébriquement clos** si tout polynôme non-constant de $K[X]$ admet au moins une racine.

Exercice 3. Montrer qu'un corps algébriquement clos est nécessairement infini (indication : penser aux polynômes de la forme $(X-a_1)\dots(X-a_r)+1$)

Théorème 1.7. Un corps K est algébriquement clos si et seulement si les seuls polynômes irréductibles de $K[X]$ sont les polynômes de degré 1.

Démonstration.

- **La condition est nécessaire :** Supposons K algébriquement clos. Tout polynôme non constant admet une racine a et est donc divisible par $X-a$. S'il n'est pas de degré 1, alors il n'est pas irréductible.
- **La condition est suffisante :** Supposons que tout polynôme irréductible est vde degré 1. Soit P un polynôme non-constant : tous les facteurs (unitaires) de sa décomposition en facteurs irréductibles sont de degré 1, et donc de la forme $X-a$. Le terme constant d'un tel facteur est alors une racine de P . □

Corollaire 1.8. Si K est algébriquement clos, tout polynôme de $K[X]$ est scindé. □

Corollaire 1.9. Si K est algébriquement clos, pour qu'un polynôme P divise un polynôme Q , il faut et il suffit que toute racine de P d'ordre de multiplicité k soit aussi racine de Q d'ordre de multiplicité au moins k . □

1.4. Polynômes sur \mathbb{C}

Théorème 1.10 (Théorème de D'Alembert-Gauss, admis). Le corps des nombres complexes est algébriquement clos. □

Et donc :

Théorème 1.11. Tout polynôme P non-nul de $\mathbb{C}[X]$ s'écrit de manière unique sous la forme :

$$P(X) = a(X-z_1)^{k_1} \dots (X-z_r)^{k_r}$$

Cette expression s'appelle **décomposition de D'Alembert** du polynôme P . □

Pour traiter le cas $K = \mathbb{R}$:

Théorème - Définition 1.12. L'application σ de $\mathbb{C}[X]$ dans lui-même, défini par :

$$\sigma\left(\sum_{i=1}^n a_i X^i\right) = \sum_{i=1}^n \bar{a}_i X^i$$

est un automorphisme involutif de l'anneau $\mathbb{C}[X]$.

Les polynômes P et $\sigma(P)$ sont dits **conjugués**. On note $\bar{P} = \sigma(P)$. □

Remarquons que l'égalité $\bar{P} = P$ a lieu si et seulement si les coefficients de P sont réels.

1.5. Polynômes sur \mathbb{R} Le point est que tout polynôme de $\mathbb{R}[X]$ peut-être vu comme un polynôme de $\mathbb{C}[X]$! Simplement, être irréductible dans $\mathbb{R}[X]$ ne signifie pas l'être dans $\mathbb{C}[X]$! (Mais l'inverse est clairement vrai).

De plus, si P est réel, on a $\sigma(P) = P$. Or, σ est un automorphisme d'anneaux, donc si $P = a(X - z_1)^{k_1} \dots (X - z_r)^{k_r}$ est la décomposition de D'Alembert de P , elle est aussi égale à $P = \bar{a}(X - \bar{z}_1)^{k_1} \dots (X - \bar{z}_r)^{k_r}$. Par unicité de la décomposition, on doit avoir $\bar{a} = a$, i.e. est réel, et pour tout z_i complexe non-réel le conjugué \bar{z}_i apparaît aussi comme racine de P , avec le même ordre de multiplicité. En réarrangeant les facteurs et en associant les racines conjuguées 2-à-2, on obtient :

Théorème 1.13. Tout polynôme P non-nul de $\mathbb{R}[X]$ s'écrit de manière unique sous la forme :

$$P(X) = a(X - x_1)^{k_1} \dots (X - x_r)^{k_r} (X^2 + a_1 X + b_1)^{l_1} \dots (X^2 + a_s X + b_s)^{l_s}$$

où a et chaque a_i est un nombre réel, et chaque $X^2 + a_i X + b_i$ un polynôme de $\mathbb{R}[X]$ sans racine réelle. □

En particulier, les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle (i.e. de discriminant strictement négatif).

2. RELATIONS ALGÈBRIQUES

Nous reconsidérons à nouveau le cas où l'anneau A est un anneau (commutatif) quelconque, et non pas un corps.

2.1. Anneau des polynômes à plusieurs indéterminées

2.1.1. Définition

Définition 2.1. Soit n un entier ≥ 1 . Un **polynôme à n indéterminées sur A** est une famille presque nulle d'éléments de A indexée par \mathbb{N}^n . L'ensemble des polynômes à n indéterminées sur A est noté $A[X_1, \dots, X_n]$

De manière similaire à ce qui est fait pour les polynômes à une indéterminée, on note les éléments de $A[X_1, \dots, X_n]$ sous la forme suivante :

$$P = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$$

étant sous-entendu que les a_{i_1, \dots, i_n} sont nuls si la somme $i_1 + \dots + i_n$ est plus grande qu'un entier N .

Le plus petit entier N pour lequel ceci est vrai est appelé **degré (total) de P** et noté $\deg P$ (lorsque P est nul, par convention : $\deg P = -\infty$).

Notations : Nous allons noter $\vec{i} = (i_1, \dots, i_n)$ les éléments de \mathbb{N}^n , et la somme $i_1 + \dots + i_n$ sera notée $\|\vec{i}\|$. On note aussi $X^{\vec{i}} := X_1^{i_1} \dots X_n^{i_n}$.

Les polynômes de la forme $X^{\vec{i}} := X_1^{i_1} \dots X_n^{i_n}$ sont appelés **monômes**.

Théorème - Définition 2.2. Soient $P = \sum_{\vec{i} \in \mathbb{N}^n} a_{\vec{i}} X^{\vec{i}}$, $Q = \sum_{\vec{j} \in \mathbb{N}^n} b_{\vec{j}} X^{\vec{j}}$ deux polynômes de $A[X_1, \dots, X_n]$. On note $P + Q$ le polynôme $\sum_{\vec{i} \in \mathbb{N}^n} (a_{\vec{i}} + b_{\vec{i}}) X^{\vec{i}}$. Pour tout entier $\vec{i} \in \mathbb{N}^n$, on définit $d_{\vec{i}} = \sum_{\vec{p} + \vec{q} = \vec{i}} a_{\vec{p}} b_{\vec{q}}$; alors la suite $(d_{\vec{i}})_{\vec{i} \in \mathbb{N}^n}$ est presque-nulle, donc un polynôme, qui est noté $P.Q$, et appelé **produit de P et Q** .

Le triplet $(K[X_1, \dots, X_n], +, \cdot)$ est un anneau commutatif non-nul. □

Et même, dans le cas où A est un corps K , $K[X_1, \dots, X_n]$ est naturellement muni d'une structure de K -espace vectoriel.

Tout polynôme s'écrit d'une unique manière comme combinaisons linéaire de monômes - dans le cas $A = K$, ceci signifie que les monômes forment une base du K -espace vectoriel $K[X_1, \dots, X_n]$.

2.2. Polynômes homogènes

Définition 2.3. Soit $p \in \mathbb{N}$. Un polynôme $P = \sum_{\vec{i} \in \mathbb{N}^n} a_{\vec{i}} X^{\vec{i}}$ est p -homogène si tous les coefficients $a_{\vec{i}}$ avec $\|\vec{i}\| \neq p$ sont nuls.

En d'autre terme, il s'agit d'une somme, éventuellement nulle, de monômes de degré total p . Ainsi, un polynôme p -homogène est de degré total p .

Un polynôme P est dit **homogène** s'il existe un entier p (son degré!) tel que P soit p -homogène.

La somme de deux polynômes p -homogènes est p -homogène, mais la somme de deux polynômes homogènes de degré différent n'est pas homogène!

Proposition 2.4. Le produit d'un polynôme p -homogène par un polynôme q -homogène est $(p+q)$ -homogène. \square

2.3. Plongements canoniques Nous avons déjà remarqué que tout anneau A «se plonge» naturellement dans son anneau de polynôme $A[X]$ comme sous anneau des polynômes constants, ie. de degré 0. De la même manière, A s'identifie naturellement au sous-anneau de $A[X_1, \dots, X_n]$ formé des polynômes de degré 0. Plus généralement, pour tout $k \leq n$, $A[X_1, \dots, X_k]$ s'identifie au sous-anneau de $A[X_1, \dots, X_n]$ formé des polynômes dont les coefficients de termes où apparaissent un X_i avec $i > k$ sont nuls.

En fait :

Théorème 2.5. L'application de $A[X_1, \dots, X_n][X] \rightarrow A[X_1, \dots, X_{n+1}]$ qui envoie un polynôme $P = \sum_{i \geq 0} P_i X^i$ avec $P_i = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$ sur le polynôme :

$$\sum_{(i_1, \dots, i_n, i_{n+1}) \in \mathbb{N}^{n+1}} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} X_{n+1}^{i_{n+1}}$$

est un isomorphisme d'anneaux. \square

Ce théorème signifie qu'on peut réarranger l'écriture de P en distinguant l'indéterminée X_{n+1} - en fait, on peut aussi choisir une autre des indéterminés, obtenant un résultat analogue!

On a aussi des isomorphismes d'anneaux $K[X_1, \dots, X_n] \approx K[X_1, \dots, X_k][X_{k+1}, \dots, X_n]$, et aussi $K[X_1, \dots, X_n] \approx K[X_1][X_2] \dots [X_n]$.

Ainsi, si une propriété passe d'un anneau A à son anneau de polynôme $A[X]$, elle se propage aussi de A vers $A[X_1, \dots, X_n]$. D'où :

Théorème 2.6. Si A est intègre, alors $A[X_1, \dots, X_n]$ est intègre, et les éléments inversibles de $A[X_1, \dots, X_n]$ sont les éléments de A qui sont inversibles. \square

2.3.1. Degré On a déjà défini le degré (total) d'un élément de $A[X_1, \dots, X_n]$; on a là encore, pour tout P, Q dans $A[X_1, \dots, X_n]$:

$$\deg(P+Q) \leq \sup[\deg P, \deg Q] \quad \deg(P.Q) \leq \deg P + \deg Q$$

avec égalité dans la dernière inégalité si A est intègre.

Exercice 4. Montrer qu'effectivement cette inégalité est un égalité lorsque A est intègre (indication : montrer qu'on peut se ramener au cas où les polynômes P et Q sont homogènes).

On peut aussi définir le **degré en la variable (ou indéterminée)** X_i d'un élément P de $A[X_1, \dots, X_n]$ à travers l'isomorphisme

$$A[X_1, \dots, X_n] \approx A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n][X]$$

On note $\deg_i P$ ce degré. Là encore :

$$\deg_i(P+Q) \leq \sup[\deg_i P, \deg_i Q] \quad \deg_i(P.Q) \leq \deg_i P + \deg_i Q$$

avec égalité dans la dernière inégalité si A est intègre.

2.3.2. Fonction polynomiale à plusieurs indéterminées Comme dans le cas à une seule indéterminée, on peut associer à tout élément $P = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$ de $A[X_1, \dots, X_n]$ l'application $\tilde{P} : A^n \rightarrow A$ qui envoie un n -uplet (x_1, \dots, x_n) sur $\sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}$. Cette application est appelée **fonction polynomiale (associée à P)**.

Ceci définit un morphisme d'anneaux de $A[X_1, \dots, X_n]$ vers A^{A^n} .

Théorème 2.7 (admis). Si A est un anneau intègre infini, le morphisme $P \rightarrow \tilde{P}$ est injectif. \square

2.3.3. Substitution Soit P un polynôme de $A[X_1, \dots, X_n]$, et n polynômes Q_1, \dots, Q_n de $A[Y_1, \dots, Y_p]$. On peut alors remplacer dans l'expression de P chaque occurrence de X_i par le polynôme Q_i ; le résultat est alors un polynôme de $A[Y_1, \dots, Y_p]$. Cette opération s'appelle **substitution des polynômes Q_1, \dots, Q_n aux indéterminées X_1, \dots, X_n** .

Cette opération correspond, au niveau des fonctions polynomiales, à la composition des applications $(\tilde{Q}_1, \dots, \tilde{Q}_p) : A^p \rightarrow A^n$ et $\tilde{P} : A^n \rightarrow A$.

Exemple 2.8. La substitution dans $P = X_1^2 + X_2 + X_1X_2 + 7$ par $Q_1 = Y_1^2, Q_2 = Y_1Y_2$ est :

$$(Y_1^2)^2 + Y_1Y_2 + (Y_1^2)(Y_1Y_2) + 7 = Y_1^4 + Y_1^3Y_2 + Y_1Y_2 + 7$$

2.3.4. Polynômes symétriques

Proposition 2.9. Soit s un élément du groupe symétrique S_n (ie. une permutation de $\{1, \dots, n\}$). L'application de $A[X_1, \dots, X_n]$ dans lui-même qui envoie chaque polynôme

$$P = P(X_1, \dots, X_n) = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$$

sur le polynôme :

$$s(P) = P(X_{s(1)}, \dots, X_{s(n)}) = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1, \dots, i_n} X_{s(1)}^{i_1} \dots X_{s(n)}^{i_n}$$

est un isomorphisme d'anneaux (et même d'espaces vectoriels si A est un corps).

Si s, s' sont deux éléments de S_n , on a :

$$(s \circ s')(P) = s'(s(P))$$

Enfin, si P est homogène, $s(P)$ est lui-aussi homogène. □

Définition 2.10. Un polynôme P est **symétrique** si pour toute permutation $s \in S_n$ on a $s(P) = P$.

Théorème - Définition 2.11. Dans $A[X_1, \dots, X_n]$ les n polynômes Σ_p ($1 \leq p \leq n$) définis par :

$$\Sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}$$

sont homogènes et symétriques. Ils sont appelés **polynômes symétriques élémentaires**.

En particulier :

$$\Sigma_1 = X_1 + \dots + X_n \quad \Sigma_n = X_1 \dots X_n$$

Démonstration. Chaque Σ_p est manifestement homogène, de degré p .

Soit P le polynôme de $A[X_1, \dots, X_n, Y]$:

$$P = \prod_{i=1}^n (Y - X_i)$$

Par récurrence sur n , on montre :

$$P = Y^n + \sum_{p=1}^n (-1)^p \Sigma_p Y^{n-p}$$

Or, pour toute permutation $s \in S_n$ on a manifestement, par commutativité du produit dans $A[X_1, \dots, X_n, Y]$:

$$\prod_{i=1}^n (Y - X_{s(i)}) = \prod_{i=1}^n (Y - X_i)$$

On en déduit que $s(\Sigma_p) = \Sigma_p$ pour tout p . □

Il est clair que si Q est un polynôme de $A[Y_1, \dots, Y_n]$, le polynôme $P \in A[X_1, \dots, X_n]$ obtenu en substituant dans Q les indéterminées par $\Sigma_1, \dots, \Sigma_n$ est symétrique.

Inversement :

Théorème 2.12 (admis). Tout polynôme symétrique de $A[X_1, \dots, X_n]$ s'obtient par substitution dans un polynôme de $A[Y_1, \dots, Y_n]$ des indéterminées par les polynômes symétriques élémentaires $\Sigma_1, \dots, \Sigma_n$.

2.4. Relations algébriques entre les racines d'un polynôme à une indéterminée Dans cette dernière section :

K est un corps algébriquement clos.

Définition 2.13. Un n -uplet $(\alpha_1, \dots, \alpha_n)$ d'éléments de K est un **système de racines pour un polynôme P de $K[X]$** si on peut écrire :

$$P = a(X - \alpha_1)\dots(X - \alpha_n)$$

Comme tout polynôme de $K[X]$ est scindé, tout polynôme de $K[X]$ admet un système de racines. Remarquons que les α_i ne sont pas deux-à-deux distincts! Et remarquons aussi qu'il n'y a pas un seul système de racines (sauf si P est de la forme $a(X - \alpha)^n$), puisque pour toute permutation $s \in S_n$ le n -uplet $(s(\alpha_1), \dots, s(\alpha_n))$ est lui aussi un système de racines. En fait, tout autre système de racines de P s'obtient de cette manière, en appliquant une permutation à $(\alpha_1, \dots, \alpha_n)$.

Définition 2.14. Le **symétrisé** d'un n -uplet $(\alpha_1, \dots, \alpha_n)$ d'éléments de K est n -uplet $(\sigma_1, \dots, \sigma_n)$ de K^n défini par $\sigma_p = \Sigma_p(\alpha_1, \dots, \alpha_n)$ ($1 \leq p \leq n$) où Σ_p désigne le polynôme symétrique élémentaire d'ordre p .

Comme les Σ_p sont symétriques, le symétrisé ne dépend finalement pas du choix du système de racines. Et, en effet :

Théorème 2.15. Soit P un polynôme de $K[X]$ de degré $n \geq 1$:

$$P = a_n X^n + \dots + a_{n-p} X^{n-p} + \dots + a_0, \quad a_n \neq 0$$

Alors, un n -uplet $(\alpha_1, \dots, \alpha_n)$ est un système de racines de P si et seulement si son symétrisé $(\sigma_1, \dots, \sigma_n)$ vérifie :

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, \dots, \sigma_p = (-1)^p \frac{a_{n-p}}{a_n}, \dots, \sigma_n = (-1)^n \frac{a_0}{a_n}$$

□