Leçon 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et app^{ns}.

Dans toute cette leçon, $\mathbb{K}$ désigne un corps commutatif.

I. Racines d'un polynôme

1. Définitions et premières propriétés

Définition 1.1 À tout polynôme $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, on associe la fonction polynomiale $\mathbb{K} \longrightarrow \mathbb{K}$, $x \longmapsto \sum_{k=0}^{n} a_k x^k$.

Notation 1.2 Pour $x \in \mathbb{K}$, on notera $P(x)$ l'évaluation de la fonction polynomiale associée à P, en x.

Définition 1.3 Soit $P \in \mathbb{K}[X]$. On dit que $\alpha \in \mathbb{K}$ est racine de P si $P(\alpha) = 0$.

Exemples 1.4
- un polynôme constant non nul n'admet pas de racine
- le polynôme nul a tous les éléments de $\mathbb{K}$ pour racines

Proposition 1.5 Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors α est racine de P si et seulement si $X - \alpha$ divise P dans $\mathbb{K}[X]$.

2. Multiplicité des racines

Définition 1.6 Soient $P \in \mathbb{K}[X]$ non constant, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On dit que α est une racine de multiplicité m de P si $(X-\alpha)^m$ divise P et $(X-\alpha)^{m+1}$ ne divise pas P.

Théorème 1.7 Soient $P \in \mathbb{K}[X]$, $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ deux à deux distincts et $m_1, \dots, m_r \in \mathbb{N}^*$ alors les deux assertions suivantes sont équivalentes :

(i) pour tout $k \in [\![1, r]\!]$, α_k est une racine de multiplicité m_k de P

(ii) il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = Q(X) \prod_{k=1}^{r} (X - \alpha_k)^{m_k}$ et vérifiant $Q(\alpha_k) \neq 0$ pour tout $k \in [\![1, r]\!]$

Corollaire 1.8 Soit $P \in \mathbb{K}[X]$ non nul admettant $r \geqslant 1$ racines distinctes $\alpha_1, \dots, \alpha_r$ de multiplicité m_k alors $\deg P \geqslant \sum_{k=1}^{r} m_k$.

En particulier, si P est de degré $n \in \mathbb{N}^*$ alors P admet au plus n racines distinctes ou confondues dans $\mathbb{K}$.

Corollaire 1.9 Si le corps $\mathbb{K}$ est infini et que $P(x) = 0$ pour tout $x \in \mathbb{K}$, $P = 0$.

Contre-exemple 1.10
Si $\mathbb{K} = \mathbb{Z}_3$, $P(X) = X(X-\bar{1})(X-\bar{2}) \neq 0$ a pour fonction polynomiale associée la fonction nulle

Théorème 1.11 On suppose que le corps $\mathbb{K}$ est de caractéristique nulle. Pour $P \in \mathbb{K}[X] \setminus \{0\}$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$, les assertions suivantes sont équivalentes :

(i) α est une racine d'ordre m de P

(ii) $\forall k \in [\![0, m-1]\!]$, $P^{(k)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$

3. Polynômes irréductibles

Définition 1.12 Un polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ est dit irréductible s'il est non inversible et n'est divisible que par les polynômes associés à P.

Exemple 1.13
- $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$
- $X^2 + 1$ est réductible dans $\mathbb{C}[X]$

Remarque 1.14 Un polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ irréductible n'admet pas de racine.

Proposition 1.15 On note μ la fonction de Mobius. Soit f une fonction multiplicative alors pour tout $n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} \mu(d)\, g\!\left(\frac{n}{d}\right)$ où $g(k) = \sum_{d'|k} f(d')$.

Proposition 1.16 On se place dans $\mathbb{F}_q$, tout diviseur irréductible de $X^{q^n} - X$ est de degré divisant n. Réciproquement, pour tout diviseur d de n, tout polynôme irréductible unitaire de degré d divise $X^{q^n} - X$.

Théorème 1.17 Pour tout $n \in \mathbb{N}^*$, on notant $I_n(q)$ le nombre de polynômes irréductibles unitaires, $I_n(q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$.

développement 1

II - Extension de corps et adjonction de racines

1. Adjonction de racines

Définition 2.1 On dit qu'un polynôme $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$, s'il est constant ou de degré $n \geq 1$ et admet n racines (en comptant les multiplicités).

Si toutes les racines de P sont de multiplicité 1, on dit que P est scindé à racines simples.

Définition 2.2 On dit que $\mathbb{K}$ est algébriquement clos si tout polynôme $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$.

Théorème 2.3 Le corps $\mathbb{C}$ est algébriquement clos.

Proposition 2.4 L'anneau $\mathbb{K}[X]/(P)$, pour $P \in \mathbb{K}[X]$ non constant, est une $\mathbb{K}$-algèbre de base $(1, X, \dots, X^{n-1})$ où $n = \deg P$.

Exemples 2.5

- dans $\mathbb{R}[X]$, X^2+1 est irréductible et $\mathbb{R}[X]/(X^2+1)$ est un corps isomorphe à $\mathbb{C}$
- dans $\mathbb{Q}[X]$, X^2-2 est irréductible et $\mathbb{Q}[X]/(X^2-2)$ est un sous-corps de $\mathbb{R}$ isomorphe à $\mathbb{Q}[\sqrt{2}]$

Définition 2.6 On dit qu'une extension $\mathbb{L}$ de $\mathbb{K}$ est un corps de rupture d'un polynôme $P \in \mathbb{K}[X]$ non constant, si P admet une racine ω dans $\mathbb{L}$.

Proposition 2.7 Soit $P \in \mathbb{K}[X]$ irréductible dans $\mathbb{K}[X]$. Alors P admet un corps de rupture, le corps $\mathbb{K}[X]/(P)$.

Corollaire - Définition 2.8 Soit $P \in \mathbb{K}[X]$ non constant. Alors, il existe une extension $\mathbb{L}$ de $\mathbb{K}$ sur laquelle P soit scindé.

On appelle $\mathbb{L}$ corps de décomposition de P ou corps des racines de P.

2. Nombres algébriques

Définition 2.9 Soient $\mathbb{K}$ et $\mathbb{L}$ des corps, $\mathbb{L}$ extension de $\mathbb{K}$. On dit que $a \in \mathbb{L}$ est un nombre algébrique s'il existe $P \in \mathbb{K}[X]$ non nul tel que $P(a) = 0$.

Proposition 2.10 Soit $a \in \mathbb{L}$ alors les assertions suivantes sont équivalentes :

(i) a est algébrique sur $\mathbb{K}$

(ii) $\mathbb{K}[a] = \mathbb{K}(a)$

(iii) $[\mathbb{K}(a) : \mathbb{K}] < +\infty$

Théorème 2.11 On note $\mathcal{A}$ l'ensemble des nombres algébriques sur $\mathbb{K}$, alors $\mathcal{A}$ est un corps dénombrable et, si $\mathbb{L}$ est algébriquement clos, $\mathcal{A}$ est algébriquement clos.

développement 2

III - Polynômes symétriques

Définition 3.1 Un polynôme $P \in A[X_1, \dots, X_n]$ est dit symétrique si pour tout $\sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Exemple 3.2

dans $\mathbb{R}[X, Y, Z]$, $P(X, Y, Z) = XY + YZ + ZX$

Définition 3.3 Soit $M = X_1^{\alpha_1} \dots X_n^{\alpha_n} \in A[X_1, \dots, X_n]$. Si $\sigma \in \mathfrak{S}_n$, on pose $M_\sigma = X_{\sigma(1)}^{\alpha_1} \cdots X_{\sigma(n)}^{\alpha_n}$. Le polynôme $\sum_{\sigma,\ M_\sigma \text{ distincts}} M_\sigma$ est symétrique dans $A[X_1, \dots, X_n]$, on l'appelle le symétrisé de M dans $A[X_1, \dots, X_n]$, noté $\sum M$.

Définition 3.4 On appelle polynômes symétriques élémentaires de $A[X_1,\dots,X_n]$ les polynômes e_k $(1 \leq k \leq n)$ définis par : $e_k = \sum X_1 \dots X_k = \sum\limits_{i_1<\dots<i_k} X_{i_1} \dots X_{i_k}$

Exemples 3.5

$e_1 = X_1 + \dots + X_n \qquad e_2 = \sum X_1 X_2 = \sum\limits_{i<j} X_i X_j \qquad e_n = X_1 \dots X_n$

Remarque 3.6 Les polynômes symétriques élémentaires vérifient l'égalité fondamentale $(T-X_1)\dots(T-X_n) = T^n - e_1 T^{n-1} + \dots + (-1)^{n-1} e_{n-1} T + (-1)^n e_n$.
En particulier, si $P = X^n + a_1 X^{n-1} + \dots + a_n$ est scindé dans $\mathbb{K}$ et si $r_1,\dots,r_n$ sont les racines, pour $k \in [\![1,n]\!]$, $a_k = (-1)^k e_k(r_1,\dots,r_n)$.

Théorème 3.7 (admis) Soient A un anneau commutatif unitaire et P un polynôme de $A[X_1,\dots,X_n]$ symétrique. Il existe alors un unique polynôme Q tel que $P = Q(e_1,\dots,e_n)$.

Exemples 3.8

- $X_1^2 + X_2^2 = e_1^2 - 2e_2$ dans $A[X_1, X_2]$
- Les sommes de Newton $S_p = \sum\limits_{i=1}^{n} X_i^p \in \mathbb{R}[X_1,\dots,X_n]$ s'exprime comme polynôme en les polynômes symétriques élémentaires, pour $p \in \mathbb{N}^*$

Théorème 3.9 (relations coefficients - racines) Soit un polynôme $P = a_0 X^n + \dots + a_{n-1} X + a_n \in \mathbb{K}[X]$ scindé dont les racines sont $r_1,\dots,r_n$. Alors pour tout $k \in [\![1,n]\!]$, $e_k(r) = (-1)^k \frac{a_k}{a_0}$ en notant $r = (r_1,\dots,r_n)$.