Soit K un corps commutatif. Si A est une K-algèbre et $P \in K[X]$, on notera encore $P : \begin{array}{l} A \longrightarrow A \\ x \longmapsto P(x) \end{array}$ la fonction polynomiale associée.

I) Racines d'un polynôme

A] Définitions et propriétés

Def 1 : Soit $K \hookrightarrow L$ une extension de corps et soit $P \in K[X]$. $a \in L$ est une racine de P si $P(a) = 0$.

Ex 2 : Pour $n \in \mathbb{N}^*$, les racines de $X^n - 1$ dans $\mathbb{C}$ sont les $e^{\frac{2ik\pi}{n}}$, $k \in [\![0, n-1]\!]$.

Prop 3 : Soient $P \in K[X]$ et $a \in K$. a est racine de P si et seulement si $(X-a) \mid P$.

Def 4 : Soient $P \in K[X]$, $a \in K$, $h \in \mathbb{N}^*$. a est une racine d'ordre h de P si $(X-a)^h \mid P$ et $(X-a)^{h+1} \nmid P$.

Prop 5 : a est racine d'ordre h si et seulement si $\forall k \in [\![0;h]\!]$ $P^{(k)}(a) = 0$ et $P^{(h+1)}(a) \neq 0$ où $P^{(k)}$ est le k-ème polynôme dérivé de P.

Prop 6 : Soient $P \in K[X]$, $a_1, \dots, a_r$ des racines 2 à 2 distinctes d'ordre $h_1, \dots, h_r$. Alors il existe $Q \in K[X]$ tel que :
$P(X) = \prod_{i=1}^{r} (X-a_i)^{h_i} Q(X)$ et $\forall i \in [\![1;r]\!]$, $Q(a_i) \neq 0$.

Cor 7 : Si $P \in K[X]$ est de degré $n \in \mathbb{N}^*$, alors P admet au plus n racines dans K.

Rem 8 : Ceci n'est plus vrai dans un anneau. Par exemple, dans $\mathbb{Z}/8\mathbb{Z}$, $P(X) = 4X$ admet 0, 2 et 4 comme racines.

Prop 9 : Soit $P \in K[X]$. Si P admet une infinité de racines, alors P est le polynôme nul.

Def 10 : $P \in K[X]$ est dit scindé sur K s'il se décompose en produit de polynômes de degré 1 de $K[X]$.

Ex 11 : $X^n - 1$ est scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$.

B] Extension de corps par adjonction de racines

Def 12 : Soit $P \in K[X]$ irréductible. Une extension $K \hookrightarrow L$ est un corps de rupture de P si il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $P(\alpha) = 0$.

Ex 13 : $\mathbb{C}$ est un corps de rupture de X^2+1 sur $\mathbb{R}$.

Thm 14 : Tout polynôme irréductible admet un corps de rupture, unique à isomorphisme près.

Thm 15 : $P \in K[X]$ est irréductible si et seulement si P n'admet aucune racine dans les extensions $K \hookrightarrow L$ telles que $[L:K] \leq \frac{n}{2}$ où $n = \deg P$.

Def 16 : Un corps de décomposition de $P \in K[X]$ est une extension $K \hookrightarrow L$ telle que P soit scindé sur L, et L est engendré sur K par les racines de P.

Thm 17 : Tout polynôme de $K[X]$ admet un corps de décomposition, unique à isomorphisme près.

App 18 : Soient $n \in \mathbb{N}^*$, $p \in \mathbb{N}$ premier et $q = p^n$. Alors il existe un unique corps à q éléments à isomorphismes près, qui est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$.

C] Eléments algébriques, transcendants

Soit $K \hookrightarrow L$ une extension de corps.

Prop-def 19 : Soit $\alpha \in L$. On pose $I(\alpha) = \{P \in K[X] \mid P(\alpha) = 0\}$. C'est un idéal de $K[X]$ qui est principal. Si $I(\alpha) = \{0\}$, α est dit transcendant sur K. Sinon, il est dit algébrique et $I(\alpha)$ est engendré par un polynôme irréductible unitaire appelé polynôme minimal de α, noté $\Pi(\alpha, K)$.

Prop 20 : Si $\alpha \in L$ est transcendant sur K, alors $K[\alpha] \simeq K[X]$ et $K(\alpha) \simeq K(X)$. En particulier, $K(\alpha) \neq K[\alpha]$.

Prop 21 : Soit $\alpha \in L$. Les assertions suivantes sont équivalentes :

⊛ α est algébrique sur k

⊛ $k[\alpha] \simeq k(\alpha)$

⊛ $\dim_k k[\alpha] < +\infty$

et dans ce cas, $\dim_k k(\alpha) = [k(\alpha):k] = \deg \operatorname{Irr}(\alpha, k)$.

DEV 1

Thm 22 : (de Gauss) Le polygone régulier à $n \in \mathbb{N}^*$ côtés est constructible si et seulement si $n = 2^{\alpha} p_1 \dots p_r$ où $\alpha \geq 1$ et $p_1, \dots, p_r$ des nombres premiers de Fermat distincts.

Thm-def 23 : k est dit algébriquement clos s'il vérifie une des propriétés équivalentes suivantes :

⊛ Tout polynôme de $k[X]$, de degré supérieur à 1, admet une racine dans k.

⊛ Tout polynôme de $k[X]$ est produit de polynômes de degré 1.

⊛ Les irréductibles de $k[X]$ sont les $X - a$, $a \in k$.

⊛ Si $k \hookrightarrow L$ est une extension algébrique (tout élément de L est algébrique sur k) alors $k \simeq L$.

Ex 24 : $\mathbb{C}$ est algébriquement clos (théorème de d'Alembert-Gauss)

Def 25 : On dit que $\bar{K}$ est une clôture algébrique de k si $k \hookrightarrow \bar{K}$ est une extension algébrique et $\bar{K}$ est algébriquement clos.

Thm 26 : (de Steinitz) Tout corps admet une clôture algébrique.

II) Polynômes symétriques

Soit A un anneau commutatif intègre et $n \in \mathbb{N}^*$.

A] Définition et polynômes symétriques élémentaires

Prop 27 : Le groupe symétrique S_n agit sur $A[X_1, \dots, X_n]$ via : $\forall f \in A[X_1, \dots, X_n]$, $\forall \sigma \in S_n$, $\sigma \cdot f = f_\sigma$ où $f_\sigma(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$.

Def 28 : Un polynôme $f \in A[X_1, \dots, X_n]$ est dit symétrique s'il est invariant sous cette action : $\forall \sigma \in S_n$, $f_\sigma = f$.

Ex 29 : $D(X_1, \dots, X_n) = \prod_{i<j} (X_i - X_j)^2$ est un polynôme symétrique appelé discriminant.

Thm-def 30 : Soit $k \in [\![1;n]\!]$. On pose :

$$\Sigma_k(X_1, \dots, X_n) = \sum_{1 \leq i_1 < \dots < i_k \leq n} \prod_{j=1}^{k} X_{i_j}.$$

Les Σ_k sont appelés polynômes symétriques élémentaires. Ce sont des polynômes symétriques.

Prop 31 : Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$, $a_n \neq 0$, de racines $x_1, \dots, x_n$ dans un corps de décomposition. Alors : $\forall k \in [\![1;n]\!]$, $\Sigma_k(x_1, \dots, x_n) = (-1)^k \frac{a_{n-k}}{a_n}$. Ce sont les relations coefficients-racines.

B] Structure des polynômes symétriques

Def-Prop 32 : Soient $M = X_1^{i_1} \dots X_n^{i_n}$ et $M' = X_1^{j_1} \dots X_n^{j_n}$ deux monômes de $A[X_1, \dots, X_n]$. On dit que M est plus haut que M' et on note $M \geq M'$ si $M = M'$ ou que le premier élément non nul de $(i_1 - j_1, \dots, i_n - j_n)$ est positif. Ceci définit une relation d'ordre total sur l'ensemble des monômes unitaires de $A[X_1, \dots, X_n]$.

Rem 33 : On définit de même $M \geq M'$ dans le cas où les monômes ne sont plus unitaires.

Def 34 : Soit $P \in A[X_1, \dots, X_n]$. On appelle monôme directeur de P le plus grand monôme de P pour cette relation, noté $MD(P)$.

Prop 35 : $\forall P, Q \in A[X_1, \dots, X_n]$, $MD(PQ) = MD(P)MD(Q)$.

Lem 36 : Soit $P \in A[X_1, \dots, X_n]$ symétrique. Alors $MD(P)$ s'écrit $MD(P) = a X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$ avec $k_1 \geq k_2 \geq \dots \geq k_n$.

Lem 37 : Soient $l_1, \dots, l_n \in \mathbb{N}$ et $l = \sum_{i=1}^{n} l_i$. Alors :

$$MD\left(\prod_{i=1}^{n} \Sigma_i^{l_i}\right) = X_1^{l} X_2^{l-l_1} X_3^{l-l_1-l_2} \dots X_n^{l_n}.$$

Thm 38 : Soit $P \in A[X_1, \dots, X_n]$ symétrique. Alors il existe un unique $Q \in A[X_1, \dots, X_n]$ tel que $P = Q(\Sigma_1, \dots, \Sigma_n)$.

[4] Cor 39 : Soient $P \in k[X_1,\dots,X_n]$ de racines $x_1,\dots,x_n$ dans une clôture algébrique. Alors $\forall Q \in k[X_1,\dots,X_n]$ symétrique, $Q(x_1,\dots,x_n) \in k$.

III) Algèbre linéaire et cyclotomie

A] Application à la réduction

Soit E un k-espace vectoriel de dimension $n \in \mathbb{N}^*$. Soit $f \in \mathcal{L}(E)$, $f \neq 0$.

[3] Prop-def 40 : L'idéal des polynômes annulateurs de f n'est pas réduit à $\{0\}$. On appelle polynôme minimal de f, noté π_f, le générateur unitaire de cet espace.

Thm 41 : $\forall \lambda \in Sp(f)$, $\forall P \in k[X]$ annulateur de f, $P(\lambda) = 0$

Thm 42 : Les valeurs propres de f sont exactement les racines de π_f.

Thm 43 : f est diagonalisable si et seulement si π_f est scindé dans k à racines simples.

Thm 44 : f est trigonalisable si et seulement si π_f est scindé dans k.

B] Localisation des racines

Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ unitaire ($a_n = 1$).

[1] Def 45 : On appelle matrice compagnon de P la matrice :

$$A_P = \begin{pmatrix} 0 & & 0 & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & 0 & \vdots \\ 0 & & 1 & -a_{n-1} \end{pmatrix}$$

Prop 46 : Le polynôme caractéristique de A_P est P.

Rem 47 : La recherche des racines de P devient donc une recherche de valeurs propres.

Thm 48 : (de Gershgorin-Hadamard) Soit $A = (a_{ij})_{1 \leq i,j \leq n}$ une matrice complexe. Soit $\lambda \in Sp_{\mathbb{C}}(A)$. Alors : [3]

$$\exists i \in [\![1,n]\!],\ |\lambda - a_{ii}| \leq \sum_{\substack{j=1 \\ j \neq i}}^{n} |a_{ij}|$$

Cor 49 : Si λ est une racine de P, alors $|\lambda| \leq 1 + \max_{0 \leq i \leq n-1} |a_i|$

+DEV 2 Comptage des racines via une forme quadratique

C] Polynômes cyclotomiques

Soient $n \in \mathbb{N}^*$. On pose $\mu_n(\mathbb{C}) = \{ e^{\frac{2ik\pi}{n}} \mid k \in [\![0;n]\!] \}$ les racines de $X^n - 1$.

Def 50 : $\omega \in \mu_n(\mathbb{C})$ est dit primitif si il engendre $(\mu_n(\mathbb{C}), \times)$. On note $\mu_n^*(\mathbb{C})$ l'ensemble des racines primitives et on appelle n-ème polynôme cyclotomique : $\Phi_n(X) = \prod_{\omega \in \mu_n^*(\mathbb{C})} (X - \omega)$ [2]

Ex 51 : Si $p \in \mathbb{N}^*$ est premier, $\Phi_p(X) = \sum_{i=0}^{p-1} X^i$.

Prop 52 : $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.

Cor 53 : $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.

App 54 : Il existe une infinité de nombres premiers p tels que $p \equiv 1 [n]$ (progression arithmétique faible de Dirichlet)

Thm 55 : (de Kronecker) Soit $P \in \mathbb{Z}[X]$ unitaire, $P(0) \neq 0$, dont les racines complexes sont de modules inférieures à 1. Alors ses racines sont des racines de l'unité. [3]

Cor 56 : Si $P \in \mathbb{Z}[X]$ est unitaire irréductible tels que ses racines sont de modules inférieurs à 1, alors $P = X$ ou P est un polynôme cyclotomique.

Références :

- Algèbre (Gourdon) [1]
- Cours d'algèbre (Perrin) [2]
- Maths pour l'agrégation (Rombaldi) [3]
- Eléments de théorie des anneaux (Calais) [4]
- Algèbre 1 (Fresnel) [5]
- Théorie des corps (Carrega) [6]