Chapitre 10. Polynômes

I. Polynômes à une indéterminée

I.1. Polynômes à coefficients dans un anneau

Si A est un anneau commutatif, $A[X]$ est un anneau commutatif pour les l.c.i. $+$ et $\times$. Et un A-module pour la l.c.i $+$ et la l.c.e. $\cdot$. $A[X]$ est une A-algebre. (vérifier)

Tout polynôme s'écrit $P(X) = a_m X^m + \cdots + a_1 X + a_0$, avec $a_m \neq 0$, le **degré** de P est $\deg P = m$

On pose $\deg 0_{A[X]} = -\infty$

Si A est un anneau commutatif intègre, $A[X]$ est un anneau commutatif intègre.

Dans ce cas $\forall P, Q \in A[X]$ $\deg(PQ) = \deg(P) + \deg(Q)$, $\deg(P+Q) \leq \max(deg\, P, deg\, Q)$

Si A est fini, $A[X]$ est dénombrable. Si A est infini, A et $A[X]$ ont le même cardinal.

Les polynômes inversibles sur un anneau commutatif $A[X]$ sont les constantes inversibles de l'anneau. $G_{A[X]} = G_A$

Les polynômes inversibles sur un corps sont tous les polynômes constants. $G_{K[X]} = G_K = K^*$

Un polynôme $P \in A[X]$ est irréductible ssi $P = QR \Rightarrow Q$ inversible ou R inversible.

I.2. Polynômes à coefficients dans un corps K

I.2.1. Division euclidienne

Pour $A \in K[X], B \in K[X]^*$ alors $\exists\,!\,(Q,R) \in K[X]$ $A = BQ + R$ et $\deg R < \deg B$

Le polynome Q est le **quotient** de la D.E. de A par B. Le polynôme R est le **reste** de la D.E. de A par B.

Le reste peut être nul avec dans ce cas $\deg(R) = -\infty$.

Dans un anneau commutatif intègre, Pour $A \in K[X], B \in K[X]^*$ tel que B est unitaire, alors $\exists\,!\,(Q,R) \in K[X]$ $A = BQ + R$ et $\deg R < \deg B$ (vérifier)

Division selon les puissances croissantes. Pour $A \in K[X], B \in K[X], B(0) \neq 0$ alors

$\forall n \in \mathbb{N}\ \exists\,!\,(Q_n, R_n) \in K[X]$ $A = BQ_n + X^{n+1}R_n$ et $\deg Q_n \leq n$.

I.2.2. Idéaux de $K[X]$

$K[X]$ est un anneau principal, euclidien, noethérien et factoriel.

Rappels : Un polynôme divise un autre ssi son idéal engendré contient celui de l'autre. Un polynôme est irréductible dans $K[X]$ ssi son idéal engendré est maximal.

Si A et B sont deux polynômes de $K[X]$, dont l'ideal engendré est $\langle A, B\rangle = \langle D\rangle$ alors $\exists U, V \in K[X]$ $AU + BV = D$. Dans ce cas $D \sim pgcd(A,B)$ et U, V sont **des coefficients de Bézout de A, B**.

Si $A \notin K, B \notin K$, alors on peut trouver U, V tels que $\deg U \leq degB - 1$ et $\deg V \leq \deg A - 1$.

Deux polynômes A, B sont premiers entre ssi $pgcd(A,B) \sim 1$ ssi $\exists U, V \in K[X]$ $AU + BV = 1$

Deux polynômes irréductibles sont premiers entre eux ssi ils sont non proportionnels.

Lemme de Gauss. $A \wedge B = 1 \Leftrightarrow \forall C \in K[X]$ $A|BC \Rightarrow A|C$

Les ideaux premiers de $K[X]$ sont d'une part les idéaux maximaux (engendrés par un polynôme irréductible) et d'autre part l'idéal $\langle 0\rangle$.

$K_n[X] = \{P \in K[X] \mid \deg P \leq n\}$ $K_0[X] \approx K$.

Pour $P \in K[X]$ tel que $\deg P = n+1$, $K[X] = \langle P\rangle \oplus K_n[X]$ et $\mathrm{codim}_{K[X]} \langle P\rangle = \deg P = n+1$

Donc $\frac{K[X]}{\langle P\rangle}$ est toujours de dimension $\deg P$.

Pour $\alpha_0, \ldots, \alpha_n \in K$, $K[X] \to K^{n+1} : P \mapsto \big(P(\alpha_0), \ldots, P(\alpha_n)\big)$ est linéaire surjective.

Pour $\alpha_0, \ldots, \alpha_n \in K$, $K_n[X] \to K^{n+1} : P \mapsto \big(P(\alpha_0), \ldots, P(\alpha_n)\big)$ est un isomorphisme d'ev.

I.2.3. Racines d'un polynôme

Une **fonction polynôme** sur un corps K est une fonction obtenue en évaluant un polynôme de $K[X]$ c'est une fonction de la forme $\tilde{P}: K \to K: x \mapsto P(x) = \phi(P, x)$ avec $P \in K[X]$ et $\phi\left(\sum_k a_k X^k, x\right) = \sum_k a_k x^k$. L'application $K[X] \to K^K: P \mapsto \tilde{P}$ est un morphisme de K-algèbres.

Par abus d'écriture on écrira simplement si $a \in K$, $P(a) = \tilde{P}(a) = \phi(P, a)$.

Un point $a \in K$ etant fixé, le morphisme $K[X] \to K: P \mapsto P(a)$ est le **morphisme d'évaluation au point fixé** a. Le morphisme d'évaluation en un point fixé, est un morphisme de K-algebres.

Une **racine/zéro** d'un polynôme de $K[X]$ est un point $a \in K$ tel que $P(a) = 0$.

Un polynôme de $K[X]$ admet une racine en un point $a \in K$ ssi ce polynome est divisible par $X - a$

Une **racine d'ordre $m \in N^*$** d'un polynôme de $K[X]$ est un point $a \in K$ ssi $(X-a)^m | P(X)$ mais pas $(X-a)^{m+1}$.

Une racine simple d'un polynôme est une racine d'ordre $m = 1$.

Tout $a \in K$ est racine d'ordre ∞ du polynome nul $0_{K[X]}$

Si un polynome de $K[X]$ est de degré n, le nombre de racines comptées avec leur multiplicité est $\leq n$.

Dans un anneau intègre, c'est encore vrai car $A[X]$ s'injecte dans $Frac(A[X])$

Dans un anneau en général c'est faux : $2X$ dans $\frac{Z}{6Z}[X]$ admet $2 > \deg(2X) = 1$ racines distinctes.

Pour un corps K infini, le morphisme $P \mapsto \tilde{P}$ est injectif : A une fonction polynomiale ne peut correspondre qu'un seul polynôme. Autrement dit si P a une infinite de racines alors $P = 0$.

Polynôme dérivé. Si $P(X) = \sum_{k=0}^{n} a_k X^k$ alors on définit $\boldsymbol{P'(X)} = \sum_{k=0}^{n-1}(k+1)a_{k+1}X^k$

On définit la dérivée nième : $\boldsymbol{P^{(n)}} = \left(P^{(n-1)'}\right)$

L'application $K[X] \to K[X]: P \mapsto P'$ est linéaire.

Si $P = \lambda \prod_{i=1}^{p}(X-\alpha_i)^{n_i}$ est scindé sur K (α_i distincts), $P' = \lambda \sum_{i=1}^{p} n_i (X-\alpha_i)^{n_i-1} \prod_{\substack{j=1 \\ j\neq i}}^{p}\left(X-\alpha_j\right)^{n_j}$

Si $P = \lambda \prod_{i=1}^{p}(X-\alpha_i)^{n_i}$ est scindé sur K, $\frac{P'}{P} = \sum_{i=1}^{p} \frac{n_i}{X-\alpha_i}$

Si $P = \lambda \prod_{i=1}^{p}(X-\alpha_i)^{n_i}$ est scindé sur K, $P \wedge P' = \prod_{i=1}^{p}(X-\alpha_i)^{n_i-1}$ donc $\deg P \wedge P' = n - p$.

Si $P = \lambda \prod_{i=1}^{p}(X-\alpha_i)^{n_i}$ est scindé sur K, $\frac{P}{P \wedge P'} = \lambda \prod_{i=1}^{p}(X-\alpha_i)$. $card\, Z(P) = \deg P - \deg P \wedge P'$

Si P est irréductible sur K, $P \wedge P' = 1$.

Le pgcd de polynômes est invariant par extension de corps.

Formule Leibniz. Si $P, Q \in K[X]$ alors $(PQ)^{(n)} = \sum_{k=0}^{n} C_n^k P^{(k)} Q^{(n-k)}$

Dans un corps de caractéristique nulle, $a \in K$ est une racine d'ordre $m \in N^*$ de $P \in K[X]$ <u>ssi</u> $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$

Dans un corps de caractéristique positive p, <u>Si</u> $a \in K$ est une racine d'ordre $m \in N^*$ de $P \in K[X]$ <u>alors</u> on a $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$

I.2.4. Polynômes irréductibles dans $\boldsymbol{C[X]}$ et dans $\boldsymbol{R[X]}$

Th. D'Alembert-Gauss. Tout polynôme $P \in C[X] \setminus C_0[X]$ <u>non constant</u> admet une racine dans C.

Autrement dit tout polynôme $P = \sum_{k=0}^{n} a_k X^k \in C[X]$ peut aussi s'ecrire $P = a_n \prod_{j=1}^{n}\left(X-\alpha_j\right)$

Les polynômes irréductibles de $C[X]$ sont les polynômes de degré 1. Les idéaux maximaux de $C[X]$ sont de la forme $\langle X-a \rangle$ avec $a \in C$.

Les polynômes irréductibles de $R[X]$ sont les polynômes de degré 1 et, d'autre part les polynômes de

degré 2 dont le discriminant est négatif. Les idéaux maximaux de $R[X]$ sont donc de la forme $\langle X-a\rangle$ avec $a \in R$ ou de la forme $\langle X^2+bX+c\rangle$ avec $b,c \in R$ et $b^2-4c<0$.

Tout polynôme de $R[X]$ s'écrit sous la forme $P = a_n \prod_{j=1}^{m}(X-\alpha_j)\prod_{k=1}^{p}(X^2-(\beta_k+\overline{\beta}_k)X+\beta_k\overline{\beta_k})$

I.3. Polynômes à coefficients dans un anneau factoriel.

Soit A un anneau factoriel de corps de fractions $\mathbb{K}$.

La surjection canonique de $\pi : A \to \frac{A}{I}$ se prolonge naturellement en une application $\psi : A[X] \to \frac{A}{I}[X]$ (appliquant π aux coefficients) qui est un morphisme d'anneaux, car la surjection canonique en est un.

Le **contenu** d'un polynôme d'un anneau factoriel A, est le pgcd dans A de ses coefficients.

Un polynôme d'un anneau factoriel A est dit **primitif** ssi son contenu dans A est 1 càd ssi aucun irréductible de l'anneau A ne divise tous ses coefficients.

Un produit fini de polynômes primitifs sur un anneau factoriel, est un polynôme primitif.

Le contenu d'un produit fini de polynômes sur un anneau factoriel est le produit des contenus.

I.4. Critère d'irréductibilité des polynômes

Un polynôme de $K[X]$ de degré $= 1$ est irréductible.

Un polynôme de $K[X]$ de degré ≥ 2 irréductible, n'a pas de racine dans K.

Un polynôme de $K[X]$ de degré 2 ou 3 sans racines dans K est irréductible.

Lien irréductibilité dans $A[X]$ et dans $\mathbb{K}[X]$.

Attention : Si $P \in A[X]$ est réductible dans $A[X]$. $\exists Q,R \in A[X]\ P = QR,\ Q \notin A^\times, R \notin A^\times$.

Alors on ne peut pas dire que P est réductible dans $\mathbb{K}[X]$, car il est possible que $Q \in A^* \subseteq \mathbb{K}^\times$.

Si $P \in A[X]$ est réductible dans $A[X]$ avec facteurs de degré ≥ 1, alors il est réductible dans $\mathbb{K}[X]$.

Un polynôme constant de $A[X]$ est irréductible dans $A[X]$ ssi irréductible dans A.

Lemme de Gauss général. Un polynôme non constant de $A[X]$, est irréductible dans $A[X]$ ssi il est primitif dans A et irréductible dans $\mathbb{K}[X]$.

Un polynôme non constant de $A[X]$ non primitif dans A, est réductible dans $A[X]$.

Un polynôme $P \in A[X]$ réductible dans $\mathbb{K}[X]$ est réductible dans $A[X]$ avec facteurs (proportionnels) de degré ≥ 1.

Un polynôme unitaire non constant de $A[X]$, est irréductible dans $A[X]$ ssi irréductible dans $\mathbb{K}[X]$.

Corollaire utile du lemme de Gauss. Deux polynômes unitaires de $\mathbb{Q}[X]$, dont le produit est dans $\mathbb{Z}[X]$, s'avèrent être dans $\mathbb{Z}[X]$.

Irréductibilité dans A/I. Pour un idéal premier I d'un anneau factoriel A, de corps de fractions $\mathbb{K}$, on peut définir l'anneau quotient intègre $\frac{A}{I}$ de corps de fractions $\mathbb{L}$.

Soit $P \in A[X]$ tel que $\overline{P} \in \frac{A}{I}[X]$ est irréductible dans $\mathbb{L}[X]$ et $\deg(\overline{P}) = \deg(P)$ alors P est irréductible dans $\mathbb{K}[X]$. Si de plus P est primitif, alors P irréductible dans $A[X]$ (Gauss).

Irréductibilité dans $\mathbb{F}_p$. Soit $P \in \mathbb{Z}[X]$ tel que $\overline{P} \in \mathbb{F}_p[X]$ est irréductible dans $\mathbb{F}_p[X]$ et $\deg(\overline{P}) = \deg(P)$ alors P est irréductible dans $\mathbb{Q}[X]$. Si de plus P est primitif, alors P irréductible dans $\mathbb{Z}[X]$.

Transfert de Gauss. Si A est un anneau factoriel, alors $A[X]$ est un anneau factoriel.

Si A est un anneau commutatif alors ($A[X]$ est principal ssi A est un corps)

Critère d'Eisenstein. Soit $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$

S'il existe un facteur irréductible $p \in A$ de valuation 1 dans a_0 ($p^2 \nmid a_0$), et tel que p divise tous les a_j sauf a_n qu'il ne divise pas, alors P est irréductible dans $\mathbb{K}[X]$.

Si de plus P est primitif, alors P irréductible dans $A[X]$ (Gauss).
Exemple : $\forall n \in N, \forall p$ premier, $X^n - p$ est irréductible dans $Q[X]$ et dans $Z[X]$.
Si p premier, $\phi_p(X) = \frac{X^p-1}{X-1}$ est irréductible dans $Q[X]$. (l'astuce typique est Eisenstein sur $\phi_p(X+1)$)
$X^4 + 1$ est réductible dans $R[X]$, irréductible dans $Q[X]$ et dans $Z[X]$.

Compléments polynômes.

Algorithme de Schubert, 1780. Il existe un algorithme de factorisation dans $Z[X]$. Montre que la question $P \in Z[X]$ est-il irréductible ? est décidable. En pratique peu utilisé, sauf dans un corps fini F_p.

Th. Berkelamp, 1967. TODO

I.2.5. Localisation des racines d'un polynôme

Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in C[X]$ unitaire et $r = \max(1, |a_0| + \cdots + |a_{n-1}|)$ alors P admet ses n racines (comptées avec multiplicité) dans le disque fermé $\overline{D}(0, r)$. Autrement dit toute racine de P est de module inférieur à r. Ainsi en dehors pour $x > r$, $P(x)$ n'est jamais nul.
Si $P \in R[X] \setminus R_0[X]$ non constant alors $\boldsymbol{P_s} = \frac{P(X)}{pgcd(P(X),P'(X))}$ a les mêmes racines que P, et n'a que des racines simples dans R ou C.
Pour un polynôme $P \in R[X]$ sans racines multiples dans C, on pose $P_0 = P, P_1 = P'$, puis on ecrit les divisions euclidiennes successives $P_{k-1} = Q_k P_k + R_k$, on pose $P_{k+1} = R_k$ et on continue jusqu'au dernier polynôme non nul P_n qui est donc une constante $P_n \in R^*$.
Une telle famille $(P_0, \dots, P_n)$ est appelée **suite de Sturm**.
Dans une suite de Sturm, P_k et P_{k+1} n'ont pas de racine commune car ils sont premiers entre eux.
Soit un polynôme $P \in R[X]$ de suite de Sturm $(P_0, \dots, P_n)$, pour $x \in R$ racine d'aucun P_i, on note $\boldsymbol{W_P}(\boldsymbol{x})$ le nombre de changement de signe dans la suite $\big(P_0(x), \dots, P_n(x)\big)$. W_P est donc défini sur tout R sauf en un nombre fini de points.

Th. Sturm, 1829. Pour un polynôme $P \in R[X]$ sans racines multiples dans C, le nombre de racines réelles de P dans un intervalle $[a, b]$ est egal a $W_P(a) - W_P(b)$, lorsque $W_P(a), W_P(b)$ sont bien définis.
Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in C[X]$ unitaire et sans racines multiples et $r = \max(1, |a_0| + \cdots + |a_{n-1}|)$ alors pour $\forall \varepsilon > 0$, le nombre de racines réelles distinctes de P est $W_P(-R - \varepsilon) - W_P(R + \varepsilon)$
Pour déterminer le nb de racines réelles distinctes de $P \in R[X]$ quelconque dans un intervalle $[a, b]$ il suffit d'appliquer le th. de Sturm au polynôme P_s. On peut ensuite trouver des intervalles contenant exactement 1 racine en appliquant Sturm à nouveau sur des sous-intervalles de $[a, b]$. La multiplicité des racines peut se calculer en appliquant le théorème a P', $(P')_s$, etc.
Pour le corollaire il peut être plus pratique de calculer $\boldsymbol{W_P}(-\infty) - \boldsymbol{W_P}(\infty) \coloneqq \lim_{M\to\infty} W_P(-M) - W_P(M)$. Pour M assez grand, les signes des $P_k(\pm M)$ sont donnes par leur termes dominants.
Le nombre de racines réelles distinctes d'un polynôme est donc aussi égal a $W_P(-\infty) - W_P(\infty)$.

Polynômes orthogonaux pour un produit scalaire à poids.

Motivations : Permet de simplifier l'intégration numérique via la méthode des quadratures de Gauss.
Pour un intervalle I de $\mathbb{R}$ d'intérieur non vide, **un poids de produit scalaire sur $\boldsymbol{I}$** correspond à une application $w: I \to \mathbb{R}$ continue strictement positive, telle que $\forall n \in \mathbb{N}\ \ I \to \mathbb{R}: t \mapsto t^n w(t)$ est intégrable sur I.
Pour un poids de produit scalaire w sur un intervalle I,
$\boldsymbol{L^2_w}(\boldsymbol{I}, \mathbb{R}) = \{f: I \to \mathbb{R} \mid f \text{ mesurable et } f^2 w \text{ intégrable sur } I\}$

Le produit scalaire de poids w sur I est $L^2_w(I,\mathbb{R})^2 \to \mathbb{R}: (f,g) \mapsto \int_I fgw$

$L^2_w(I,\mathbb{R})$ est un espace de Hilbert pour ce produit scalaire.

L'ensemble des polynômes réels $\mathbb{R}[X]$ est en isomorphe aux fonctions polynômes réelles définies sur I car d'intérieur non vide, qui forment un sous espace de L^2_w.

Donc en identifiant polynôme et fonction polynôme, on considère que $\mathbb{R}[X]$ est un $\mathbb{R}$ sev de $L^2_w(I)$

La famille $(t \to t^n \in \mathbb{R}[X])_{n\in\mathbb{N}}$ est une famille libre du préhilbertien $\mathbb{R}[X] \subseteq L^2_w(I)$

On peut donc utiliser Gram-Schmidt, en une famille $(\boldsymbol{Q_n} \in \mathbb{R}[X])_{n\in\mathbb{N}}$

Donc $\forall n \in \mathbb{N}\ \ vect(1,t,\dots,t^n) = \mathbb{R}_n[X] = vect(Q_0,Q_1,\dots,Q_n)$ et $(t^n|Q_n) > 0$

$Q_n = \lambda_n t^n + \cdots + \lambda_1 t + \lambda_0$ avec $\lambda_n \neq 0$. On pose $\boldsymbol{P_n} = \frac{1}{\lambda_n} Q_n$, pour la rendre unitaire

P_n est **la famille orthonormalisée**.

Donc $(P_n)_{n\in\mathbb{N}}$ est une famille orthogonale de $\mathbb{R}[X]$, et pour tout n, $\deg P_n = n$, P_n est unitaire.

$\forall n \in \mathbb{N}\ \ \mathbb{R}_n[X] = vect(P_0,P_1,\dots,P_n)$

$\forall n \in \mathbb{N}\ \ P_{n+1} \in \mathbb{R}_n[X]^\perp$

$\forall n \geq 1\ \exists a_n,b_n,c_n \in \mathbb{R}\ \ XP_n = a_nP_{n+1} + b_nP_n + c_nP_{n-1}$ de plus $c_n = a_{n-1}$

Formule de Christoffel-Darboux. $\forall n \geq 0\ \exists \boldsymbol{K_n} \in \mathbb{R}\ \forall x,y \in \mathbb{R}\ \ (x-y)\sum_{k=0}^n P_k(x)P_k(y) = K_n\big(P_{n+1}(x)P_n(y) - P_n(x)P_{n+1}(y)\big)$, $\boldsymbol{K_n}$ est le quotient des coefficients dominants de P_n et P_{n+1}

Pour $n \in \mathbb{N}^*$ P_n est admet exactement n racines distinctes dans I donc scindé simple sur I.

Pour $n \in \mathbb{N}$ entre deux racines de P_{n+1}, il y a exactement une racine de P_n.

Pour $n \in \mathbb{N}$ et $x_0 \in I$ tel que $P_n(x_0) \neq 0$, le nombre de racines de P_n supérieures à x_0 est égal au nombre de changements de signes dans la suite finie $\big(P_k(x_0)\big)_{k\leq n}$

Si w est C^1, et $\exists A,B \in \mathbb{R}[X]\ (Aw)' = Bw$, et Aw nul aux bornes de I alors $\phi: P \mapsto BP' + AP''$ est un endomorphisme auto-adjoint de $\mathbb{R}[X]$, on peut alors construire une nouvelle famille orthonormale $(R_n)_n$ telle que $\forall n \in \mathbb{N}\ R_n$ vecteur propre de ϕ et ne diffère de P_n que d'un signe, et on obtient

$\forall n \in \mathbb{N}\ \exists \mu_n \in \mathbb{R}\ A(x)P_n''(x) + B(x)P_n'(x) + \mu_n P_n(x) = 0$

puis la **formule de Rodrigues** $\forall n \in \mathbb{N}\ \exists \lambda \in \mathbb{R}\ \forall x \in I\ \ P_n(x) = \frac{\lambda}{w(x)}\frac{d^n}{dx^n}(w(x)A(x)^n)$

Exemples :

Polynômes	I	$w(t)$	Relation récurrente	Equa diff
Legendre	$]-1,1[$	1	$(n+1)P_{n+1} + (2n+1)XP_n + nP_{n-1} = 0$	$(1-x^2)y'' - xy' + n^2y = 0$
Laguerre	$\mathbb{R}_+$	e^{-t}	$(n+1)P_{n+1} + (x-2n-1)P_n + nP_{n-1} = 0$	$xy'' + (1-x)y' + ny = 0$
Tchebytchev	$]-1,1[$	$\frac{1}{\sqrt{1-t^2}}$	$P_{n+1} - 2XP_n + P_{n-1} = 0$	$(1-x^2)y'' - xy' + n^2y = 0$
Hermite	$\mathbb{R}$	e^{-t^2}	$P_{n+1} - 2XP_n + 2nP_{n-1} = 0$	$y'' - 2xy' + 2ny = 0$

Schéma d'intégration numérique : quadrature de Gauss.

Newton-Cotes : $\int_a^b f \approx (b-a)\sum_{k=0}^n \lambda_k f\left(\alpha + k\frac{b-a}{n}\right)$ avec λ_k constantes bien choisies

La quadrature de Gauss vise à améliorer Newton-cotes.

On note $(x_1,\dots,x_n)$ les n racines distinctes de P_n.

Les $\varphi_i: Q \in \mathbb{R}_{n-1}[X] \mapsto Q(x_i) \in \mathbb{R}$ sont n formes linéaires indépendantes sur $\mathbb{R}_{n-1}[X]$ donc forment une base du dual $\mathbb{R}_{n-1}[X]^\star$

Donc $\forall n \geq 1\ \exists \lambda_1, \dots, \lambda_n \in \mathbb{R}^n\ \forall Q \in \mathbb{R}_{n-1}[X]\ \ \int_I Q(x)w(x)dx = \sum_{i=1}^n \lambda_i Q(x_i)$

L'idée de la quadrature de Gauss est de considérer $\sum_{i=1}^n \lambda_i Q(x_i)$ comme approximant l'intégrale $\int_I f(x)w(x)dx$

La dernière propriété est vraie pour une famille plus grande de polynômes

$\forall n \geq 1\ \exists \lambda_1, \dots, \lambda_n \in \mathbb{R}^n\ \forall Q \in \mathbb{R}_{2n-1}[X]\ \ \int_I Q(x)w(x)dx = \sum_{i=1}^n \lambda_i Q(x_i)$

Coefficients explicites : $\forall i \in [\![1, n]\!]\ \lambda_i = -\frac{1}{K_n P_{n+1}(x_i) P_n'(x_i)}$

Erreur de la quadrature de Gauss. Pour $f: I \to \mathbb{R}$ de classe C^{2n} alors $\left|\int_I f(x)w(x)dx - \sum_{i=1}^n \lambda_i f(x_i)\right| \leq \frac{1}{\alpha_n^2 (2n)!} \sup_{u \in I} \left|f^{(2n)}(u)\right| \|P_n^2\|$ où α le coefficient dominant de P_n

Pour les polynômes de Tchebychev on trouve par exemple

Pour $f: I \to \mathbb{R}$ de classe C^{2n} alors $\int_{-1}^1 \frac{f(x)dx}{\sqrt{1-x^2}} \approx \frac{\pi}{n} \sum_{k=1}^n f\left(\cos \frac{(2k-1)\pi}{2n}\right)$

II. Polynômes à plusieurs indéterminées

II.1. Algèbre $A[X_1, \dots, X_n]$

Soit A un anneau, les anneaux $(A[X_1])[X_2]$ et $(A[X_2])[X_1]$ sont canoniquement isomorphes.

On les identifie donc et on note $A[X_1, X_2]$, par récurrence $A[X_1, \dots, X_n] = (A[X_1, \dots, X_{n-1}])[X_n]$

Un élément de $A[X_1, \dots, X_n]$ s'écrit sous la forme d'une somme finie : $\sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$

Pour $P \in A[X_1, \dots, X_n]$ on note $\deg_{X_i} P$ le degré du polynôme $(A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n])[X_i]$, c'est le **degré partiel en X_i de P**.

Un monôme de $A[X_1, \dots, X_n]$ est un terme de la forme $X_1^{i_1} \dots X_n^{i_n}$ avec $(i_1, \dots, i_n) \in N^n$.

Le degré total d'un monôme $X_1^{i_1} \dots X_n^{i_n}$ est $i_1 + \dots + i_n$

Le degré total d'un polynôme $P \in A[X_1, \dots, X_n]$ est le maximum des degrés totaux des monômes qui apparaissent dans l'écriture de P.

On peut également définir **l'anneau des polynômes a ∞ indéterminées** $A[X_1, \dots] = \cup_{n \in N} A[X_1, \dots, X_n]$

L'anneau des polynômes a n indéterminées sur un anneau factoriel, est un anneau factoriel.

L'anneau des polynômes a n indéterminées sur un anneau noethérien, est un anneau noethérien.

L'anneau des polynômes a ∞ indéterminées sur un anneau factoriel, est un anneau factoriel.

Même si A est un corps, L'anneau des polynômes a ∞ indéterminées $A[X_1, \dots]$ n'est jamais noethérien.

Donc $A[X_1, \dots]$ peut-être un exemple d'anneau factoriel non noethérien.

$\frac{Z[T]}{T^2+5}$ est un anneau intègre, noethérien mais pas factoriel.

Une **fonction polynôme a n indéterminées** sur un corps K est une fonction obtenue en évaluant un polynôme de $K[X_1, \dots, X_n]$ c'est une fonction de la forme $\tilde{P}: K^n \to K: (x_1, \dots, x_n) \mapsto P(x_1, \dots, x_n) = \phi\big(P, (x_1, \dots, x_n)\big)$ avec $P \in K[X_1, \dots, X_n]$ et

$\phi\left(\sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}, (x_1, \dots, x_n)\right) = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}$.

L'application $K[X_1, \dots, X_n] \to K^{K^n}: P \mapsto \tilde{P}$ est un morphisme de K-algèbres.

Par abus d'écriture on écrira si $a \in K^n$, $P(a) = \tilde{P}(a) = \phi(P, a)$.

Un point $a \in K^n$ etant fixé, le morphisme $K[X_1, \dots, X_n] \to K: P \mapsto P(a)$ est le **morphisme d'évaluation au point fixé** $a = (a_1, \dots a_n)$. Le morphisme d'évaluation en un point fixé, est un morphisme de K-algebres.

Si K est un corps infini, $K[X_1, \dots, X_n] \to K^{K^n} : P \mapsto \tilde{P}$ est un morphisme injectif.

II.2. Formules d'Euler et de Taylor Soit K un corps

Un polynôme $P \in K[X_1, \dots, X_n]$ est **homogène de degré $\boldsymbol{d} \in \boldsymbol{N}$** ssi tous ses monômes sont de degré d.

Dans ce cas $P(YX_1, \dots, YX_n) = Y^d P(X_1, \dots, X_n)$ dans $K[X_1, \dots, X_n, Y]$ mais réciproque fausse dans un corps fini $\mathbb{F}_p$ par exemple : $X^p - X$ vérifie la propriété pour $d = p$, mais n'est pas p homogène.

Dans un corps <u>infini</u>, un polynôme $P \in K[X_1, \dots, X_n]$ est **homogène de degré $\boldsymbol{d} \in \boldsymbol{N}$** ssi dans $K[X_1, \dots, X_n, Y]$ on a $P(YX_1, \dots, YX_n) = Y^d P(X_1, \dots, X_n)$.

La **composante homogène de degré $\boldsymbol{d} \in \boldsymbol{N}$** d'un $P \in K[X_1, \dots, X_n]$ est la somme des termes de degré total d dans l'ecriture de P, soit $P_d = \sum_{i_1+\cdots+i_n=d} a_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n}$. Elle est homogène de degré d.

Un polynôme $P \in K[X_1, \dots, X_n]$ est donc la somme de ses composantes homogenes $P = \sum_{d=0}^{\deg P} P_d$

Un polynôme <u>non nul</u> à n indeterminees sur un corps K est homogène de degré $d \in N$ ssi la seule composante homogene non nulle de P est P_d de degré d.

Th. d'Euler : Un polynôme a n indeterminees $P \in K[X_1, \dots, X_n]$ homogène de degré $q \in N$ verifie $X_1 \frac{\partial P}{\partial X_1} + \cdots + X_n \frac{\partial P}{\partial X_n} = qP$

Formule de Taylor : Sur un corps <u>de caractéristique nulle</u>, un polynôme a n indéterminées $P \in K[X_1, \dots, X_n]$ vérifie $P(X+Y) = \sum_{k=0}^{N} \frac{Y^k}{k!} P^{(k)}(X)$ avec $N = \deg P$

En caractéristique p premier, cette formule n'est pas valable sans précautions.

On a $(X+Y)^p = X^p + Y^p$ dans un corps de caractéristique p.

III. Polynômes symétriques

Sur un anneau commutatif A, le **$\boldsymbol{k}$-ième polynôme symétrique élémentaire a $\boldsymbol{n}$ indéterminées** avec $k \in \{1, \dots n\}$ est le polynome $\boldsymbol{\sigma_k} = \sum_{1 \le i_1 < \cdots < i_k \le n} X_{i_1} \dots X_{i_k} \in A[X_1, \dots, X_n]$

On a pour cas extrêmes : $\sigma_1 = X_1 + \cdots + X_n$ et $\sigma_n = X_1 \dots X_n$

Dans $A[X_1, \dots X_n, X]$ on a : $\prod_{i=1}^{n} (X - X_i) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^k \sigma_k X^{n-k} + \cdots + (-1)^n \sigma_n$

On definit $G_n \times A[X_1, \dots, X_n] : (\sigma, P) \mapsto \sigma P = P\left(X_{\sigma(1)}, \dots, X_{\sigma(n)}\right)$, c'est une action de G_n sur $A[X_1, \dots X_n]$

Un polynôme symétrique a $\boldsymbol{n}$ indéterminées de $\boldsymbol{A[X_1, \dots, X_n]}$ est un polynôme tel que $\sigma P = P$, autrement dit c'est un polynôme invariant par permutation des variables (sous l'action de G_n).

autrement dit $\forall i \neq j \quad P\left(X_1, \dots, X_i, \dots, X_j, \dots, X_n\right) = P\left(X_1, \dots, X_j, \dots, X_i, \dots, X_n\right)$

Les polynômes symétriques élémentaires sont des polynômes symétriques.

Le k-ieme polynôme symétrique élémentaire est homogène de degré k.

Tout polynôme à une variable est symétrique.

Le degré partiel d'un polynôme symétrique, est indépendant de la variable choisie, donc défini tel quel.

Pour G sous-groupe de G_n, $\boldsymbol{A[X_1, \dots, X_n]^G}$ l'ensemble des polynômes fixes par l'action de G_n, est une $\mathbb{K}$-sous- algèbre de $A[X_1, \dots, X_n]$, appelée **sous-algèbre de $\boldsymbol{A[X_1, \dots, X_n]}$ invariante par $\boldsymbol{G}$**.

Si T est une partie génératrice de G, $A[X_1, \dots, X_n]^G = \bigcap_{g \in T} A[X_1, \dots, X_n]^g$

L'ensemble des polynômes symétriques peut donc se noter $A[X_1, \dots, X_n]^{G_n}$

III.1. Relations entre coefficients et racines

Pour un polynôme <u>scindé</u> $P = \sum_{k=0}^{n} a_k X^k = a_n \prod_{j=1}^{n} \left(X - \alpha_j\right) \in K[X]$ sur un corps K, on a :

$\frac{a_{n-1}}{a_n} = -\sigma_1(\alpha_1, \dots, \alpha_n) = -\alpha_1 - \alpha_2 - \cdots - \alpha_n$

$\frac{a_{n-k}}{a_n} = (-1)^k \sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le n} \alpha_{i_1} \dots \alpha_{i_k}$

$\frac{a_0}{a_n} = (-1)^n \sigma_n(\alpha_1, \dots, \alpha_n) = (-1)^n \alpha_1 \dots \alpha_n$

III.2. Théorème de structure

Sur un anneau commutatif, le **poids d'un monôme** $X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n]$ est $i_1 + 2i_2 + \dots + ni_n$.
Le **poids d'un polynôme** $P \in A[X_1, \dots, X_n]$ est $\boldsymbol{w(P)}$ le maximum des poids des monômes intervenant dans l'écriture de P.

Le poids du k-ieme polynôme symétrique élémentaire σ_k est $w(\sigma_k) = nk - \frac{k(k-1)}{2}$

Th. de structure des polynômes symétriques. Sur un anneau commutatif A, pour un polynôme symétrique $P \in A[X_1, \dots, X_n]^{G_n}$, $\exists!\, Q \in A[X_1, \dots, X_n]$ tel que
$P(X_1, \dots, X_n) = Q\big(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n)\big)$. De plus $w(Q) \leq \deg P$

Independence des polynômes symétriques élémentaires. Les polynômes symétriques élémentaires sont algébriquement indépendants, c'est-à-dire il n'existe pas $F \in A[X_1, \dots, X_n]$ tel que
$F\big(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n)\big) = 0$. Donc dans le théorème précèdent Q est unique.
$A[X_1, \dots, X_n]^{G_n}$ est une A-algèbre de polynômes à n variables isomorphe à $A[X_1, \dots, X_n]$?
Pour un polynôme <u>unitaire</u> P sur un anneau commutatif $A[X]$, scindé dans un sur-anneau B, alors les polynômes symétriques élémentaires σ_i de ses racines $\alpha_1, \dots, \alpha_n$ sont dans A, par relations coeffs/racines. Donc pour tout $F \in A[X_1, \dots, X_n]$ <u>symétrique</u>, $F(\alpha_1, \dots, \alpha_n) \in A$. (Par th de structure).
En particulier $\forall l \in \mathbb{N}\ \ \alpha_1^l + \dots + \alpha_n^l \in A$, pour $F = X_1^l + \dots + X_n^l$.
En particulier pour $k \in \{1, \dots, n\}$ on peut construire dans A un polynôme $Q_k \in A[X]$ dont les racines sont exactement les sommes de k racines distinctes α_i de $P \in A[X]$ scindé dans un sur-anneau B.

III.3. Sommes de Newton

On appelle $\boldsymbol{k}$**-ieme somme de Newton a** $\boldsymbol{n}$ **variables**, le polynôme $\boldsymbol{S_k} = X_1^k + \dots + X_n^k \in A[X_1, \dots, X_n]^{G_n}$
La k-eme somme de Newton à n variables est un polynôme symétrique homogène de degré k.
Th. Newton. Pour $k \geq n$, $S_k - \sigma_1 S_{k-1} + \dots + (-1)^n \sigma_n S_{k-n} = 0$
Pour $k \leq n$, $S_k - \sigma_1 S_{k-1} + \dots + (-1)^k k\sigma_k = 0$
Cela permet de calculer les S_k en fonction des σ progressivement. Le théorème de structure n'est pas pratique à appliquer pour les S_k, on préfère donc le théorème de Newton pour ça.
Dans un corps K ou $k!$ est inversible, on peut utiliser les k premieres formules de Newton pour exprimer σ_k comme polynôme en fonction des $S_1, \dots, S_k$.
Dans un corps K ou $n!$ est inversible (par ex caractéristique 0), tout polynôme s'exprime de façon unique comme un polynôme en $S_1, \dots, S_n$. Dans ce cas on a $K[X_1, \dots, X_n]^{G_n} = K[S_1, \dots, S_n]$.
On pose $N(T) = \sum_{k=1}^{\infty} S_k\, T^k$, on pose $h(T) = T^n g\left(\frac{1}{T}\right) = \prod_{j=1}^{n}(1 - X_i T)$
alors $T\frac{h'(t)}{h(t)} = -N(T)$, collecter le coeff de T^k donne Q_k telle que $S_k = Q_k(\sigma_1, \dots, \sigma_n)$.
Application : M nilpotente ssi $\forall k \geq 1\ \ tr\big(M^k\big) = 0$.

IV. Elimination : Comment résoudre p equations polynomiales à n inconnues ?
Spécialité (finir plus tard si intérêt)
On s'intéresse au cas $p = 2, n = 1$

IV.1. Résultant de deux polynômes Soit K corps commutatif, $K_p[X] = \{P \in K[X] \mid \deg P \leq p\}$

Le résultant de 2 polynômes $\boldsymbol{A = \sum_{k=0}^{n} a_k X^k}$, $\boldsymbol{B = \sum_{k=0}^{n} b_k X^k \in K[X]}$ **tels que** $\boldsymbol{a_0 b_0 \neq 0}$ est

$$R(A,B)=\begin{vmatrix} a_0 & 0 & \dots & 0 & b_0 & \dots & 0 \\ a_1 & a_0 & \dots & 0 & b_1 & \dots & 0 \\ \dots & a_1 & \dots & 0 & \dots & \dots & b_0 \\ a_m & \dots & \dots & a_0 & \dots & \dots & b_1 \\ 0 & a_m & \dots & a_1 & b_n & \dots & \dots \\ 0 & 0 & \dots & \dots & 0 & \dots & \dots \\ 0 & 0 & \dots & a_m & 0 & \dots & b_n \end{vmatrix} \in K[a_0,\dots,a_m,b_0,\dots,b_n]$$

C'est un **déterminant de Sylvester**. Il est d'ordre $m+n$.

Le pgcd de deux polynômes de $K[X]$ est de degré ≥ 1 ssi leur résultant $R(A,B)$ est nul.

Sur un corps K algebriquement clos, deux polynômes de $K[X]$ ont une racine commune ssi $R(A,B)=0$

Pour 2 polynômes <u>scindés</u> $A=\sum_{k=0}^{n} a_k X^k = a_n \prod_{j=1}^{n}(X-\alpha_j), B=\sum_{k=0}^{n} a_k X^k = b_n \prod_{j=1}^{n}(X-\beta_j) \in K[X]$ sur un corps K alors $R(A,B)=a_n^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i-\beta_j)=a_n^n \prod_{i=1}^{m} B(\alpha_i)=(-1)^{mn}R(B,A)$

Dans $K[X]$, pour 3 polynomes A, B_1, B_2 on a $R(A,B_1,B_2)=R(A,B_1)R(A,B_2)$

IV.2. Applications algébriques du résultant

IV.2.1. Racines multiples des polynômes

IV.2.2. Nombres algébriques

IV.2.3. Transformation des équations algébriques

IV.2.4. Application arithmétique

V. Fractions rationnelles

V.1. Corps $K[X]$ des fractions rationnelles

Le corps des fractions rationnelles sur un corps K est l'ensemble $\boldsymbol{K(X)}=Frac(K[X])$

On a donc $\forall \frac{A}{B},\frac{C}{D} \in K(X)$ $\frac{A}{B}+\frac{C}{D}=\frac{AD+BC}{BD}$ et $\frac{A}{B}\times\frac{C}{D}=\frac{AC}{BD}$, $(K(X),+,\times)$ est un corps commutatif.

On peut identifier $K[X]$ a son plongement $K[X]\subset K(X)$ via l'injection $A\mapsto\frac{A}{1}$.

Tout fraction rationnelle F sur un corps K, admet un unique représentant $\frac{A}{B}$ avec $A\wedge B=1$ et B unitaire.

C'est le **représentant irréductible de la fraction F.**

Une **racine = zéro de multiplicité $\boldsymbol{m}\in\boldsymbol{N}^*$ d'une fraction rationnelle** $F=\frac{A}{B}$ avec $A\wedge B=1$, est une racine de multiplicite m de son **numérateur** A.

Un **pôle de multiplicité $\boldsymbol{m}\in\boldsymbol{N}^*$ d'une fraction rationnelle** $F=\frac{A}{B}$ avec $A\wedge B=1$, est une racine de multiplicite m de son **dénominateur** B.

L'ensemble de définition d'une fraction rationnelle $F=\frac{A}{B}$ avec $A\wedge B=1$ est l'ensemble $\boldsymbol{D(F)}$ égal au corps K privé des pôles de la fraction.

Une **fonction rationnelle** sur un corps K est une fonction obtenue en évaluant une fraction rationnelle de $K(X)$ c'est une fonction de la forme $\tilde{F}: D(F)\to K: x\mapsto F(x)=\phi(F,x)$ avec $F\in K(X)$ et $\phi\left(F=\frac{A}{B},x\right)=\frac{\tilde{A}(x)}{\tilde{B}(x)}$.

Par abus d'écriture on écrira simplement si $a\in D(F)$, $F(a)=\tilde{F}(a)=\frac{\tilde{A}(a)}{\tilde{B}(a)}=\frac{A(a)}{B(a)}=\phi(F,a)$.

Sur un corps infini, deux fonctions rationnelles qui coïncident sur l'intersection de leur ensemble de définition, correspondent à la même fraction rationnelle. (Injectivité).

On appelle **degré d'une fraction rationnelle $\boldsymbol{F=\frac{A}{B}}$** le nombre $\deg F=\deg A-\deg B$, ce nombre est

indépendant du représentant $\frac{A}{B}$ choisi. $\deg 0 = -\infty$

Pour 2 fractions rationnelles on a

$\deg(FG) = \deg(F) + \deg(G)$, $\deg(F+G) \leq \max(deg(F), deg(G))$ et si $\deg(F) \neq \deg(G)$, alors $\deg(F+G) = \max(deg(F), deg(G))$.

Pour toute fraction rationnelle $F = \frac{A}{B} \in K(X)$ sur un corps, il existe un unique polynome $E \in K[X]$ tel que $\deg(F-E) < 0$. On appelle E, la **partie entière de la fraction rationnelle F**, et $\boldsymbol{E(F)} = E$

V.2. Décomposition en éléments simples

V.2.1. Cas général

Soit $\boldsymbol{I}(\mathbb{K})$ l'ensemble des polynômes de $\mathbb{K}[X]$ irréductibles et unitaires sur un corps $\mathbb{K}$

$\mathbb{K}[X]$ est un espace vectoriel dont $B = (X^n)_{n\in\mathbb{N}}$ est un base

$\mathbb{K}(X)$ est un espace vectoriel dont $B = \left((X^n)_{n\in\mathbb{N}}, \left(\frac{X^m}{P^l}\right)_{P\in I(\mathbb{K}), l\in\mathbb{N}^*, 0\leq m<\deg P}\right)$ est une base

$\forall F \in \mathbb{K}(X)\ \exists!\, E \in \mathbb{K}[X]\ \exists!\, \left(a_{P,l,m}\right)_{P,l,m}$ presque tous nuls $F = E + \sum_{P\in I(\mathbb{K})} \sum_{l\in\mathbb{N}^*} \frac{\sum_{m=0}^{\deg P-1} a_{P,l,m} X^m}{P^l}$

Forme utile. Soit $F \in \mathbb{K}(X)$, $F = \frac{N}{D}$ avec $N \wedge D = 1$, D unitaire. Alors on peut décomposer en facteurs irréductibles $D = D_1^{m_1} \dots D_n^{m_n}$ avec $D_1, \dots, D_n \in I(\mathbb{K})$, $m_1, \dots, m_n \in \mathbb{N}^*$.

Alors $\exists!\, E \in \mathbb{K}[X]\ \exists!\, \left(A_{i,j} \in \mathbb{K}[X]\right)_{\substack{1\leq i\leq n \\ 1\leq j\leq \alpha_i}} \mid \deg A_{i,j} < \deg D_i$ et $F = E + \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{A_{i,j}}{D_i^j}$

E s'avère être la partie entière de F.

On appelle $A_{i,j}$ **la partie polaire de $\boldsymbol{F}$ associée a $\boldsymbol{(i,j)}$,** $\sum_{j=1}^{m_i} \frac{A_{i,j}}{D_i^j}$ **la partie polaire de $\boldsymbol{F}$ associée a $\boldsymbol{i}$, et** $\sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{A_{i,j}}{D_i^j}$ **la partie polaire de $\boldsymbol{F}$**.

V.2.2. Décomposition en éléments simples dans un corps algébriquement clos $\mathbb{C}$

$\mathbb{C}(X)$ est un espace vectoriel dont $B_{\mathbb{C}(X)} = \left((X^n)_{n\in\mathbb{N}}, \left(\frac{1}{(X-a)^l}\right)_{a\in\mathbb{C}, l\in\mathbb{N}^*}\right)$ est une base

$\forall F \in \mathbb{C}(X)\ \exists!\, E \in \mathbb{C}[X]\ \exists!\, \left(c_{a,l}\right)_{a\in\mathbb{C}, l\in N^*}$ $F = E + \sum_{a\in\mathbb{C}} \sum_{l\in\mathbb{N}^*} \frac{c_{a,l}}{(X-a)^l}$, avec $c_{a,l}$ presque tous nuls.

Forme utile. Soit $F \in \mathbb{C}(X)$, $F = \frac{N}{D}$ avec $N \wedge D = 1$, D unitaire. Alors on peut décomposer en facteurs irréductibles $D = \prod_{i=1}^{n} (X-\alpha_i)^{m_i}$ avec $\alpha_1, \dots, \alpha_n \in \mathbb{C}$, $m_1, \dots, m_n \in \mathbb{N}^*$.

Alors $\exists!\, E \in \mathbb{C}[X]\ \exists!\, \left(c_{i,j} \in \mathbb{C}\right)_{\substack{1\leq i\leq n \\ 1\leq j\leq \alpha_i}}$ et $F = E + \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{c_{i,j}}{(X-\alpha_i)^j}$

On cherche ensuite à déterminer les coefficients $c_{i,j}$.

Pour un <u>pôle simple</u> α_i on a $c_{i,1} = \frac{N(\alpha_i)}{D'(\alpha_i)}$ et en écrivant $D = (X-\alpha_i)D_1$, on a aussi $c_{i,1} = \frac{N(\alpha_i)}{D_1(\alpha_i)}$

Pour un <u>pôle multiple</u> α_i d'ordre $h \geq 2$, écrivant $D = (X-\alpha_i)^h D_1$, on a $F = \frac{N}{(X-\alpha_i)^h D_1}$

En posant $T = X - \alpha_i$, et en faisant la division selon les puissances croissantes de N par D_1 à l'ordre $h-1$, on obtient $N = \left(a_1(X-\alpha_i)^{h-1} + \dots + a_{h-1}(X-\alpha_i) + a_h\right)D_1 + (X-\alpha_i)^h S$ avec $S \in \mathbb{C}[X], S(\alpha_i) \neq 0$. On obtient $F = \frac{a_1}{X-\alpha_i} + \dots + \frac{a_h}{(X-\alpha_i)^h} + \frac{S}{D_1}$ donc la partie polaire associée à α_i.

Exemple $F = \frac{X+3}{(X-1)^4(X+1)} = \frac{N_1}{(X-1)^4 D_1}$ on pose $T = X-1$, on fait

$X + 3 = 4 + T$ | $X + 1 = 2 + T$

$-2(2+T) = -T$

$-\left(-\frac{1}{2}T\right)(2+T) = \frac{T^2}{2}$

$-\left(\frac{1}{4}T^2\right)(2+T) = -\frac{T^3}{4}$

$-\left(-\frac{1}{8}T^3\right)(2+T) = \frac{T^4}{8}$

$2 - \frac{1}{2}T + \frac{1}{4}T^2 - \frac{1}{8}T^3$

On s'arrête à l'ordre $h-1=3$

Donc $X+3 = (X+1)\left(2 - \frac{(X-1)}{2} + \frac{(X-1)^2}{4} - \frac{(X-1)^3}{8}\right) + \frac{(X-1)^4}{8}$

Donc $F = \frac{X+3}{(X-1)^4(X+1)} = -\frac{1}{8(X-1)} + \frac{1}{4(X-1)^2} - \frac{1}{2(X-1)^3} + \frac{2}{(X-1)^4} + \frac{1}{8(X+1)}$

En pratique on utilise la formule pour les pôles simples, mais pas pour les pôles multiples.

On préfère utilise des méthodes astucieuses exploitant les propriétés de F, comme la parité, les limites, la conjugaison, partie réelle/imaginaire, etc…

Pour une fraction rationnelle complexe $F \in \mathbb{C}(X)$ sans pôle dans $\mathbb{N}$, $\sum_{n\geq 0} F(n)z^n$ est de rayon 1.

Pour $k \in \mathbb{N}$ $\sum_{n\geq 0}\binom{n+k}{k}z^n$ est de rayon de convergence 1. Et $\sum_{n=0}^{\infty}\binom{n+k}{k}z^n = \frac{1}{(1-z)^{k+1}}$

Pour une fraction rationnelle complexe $F \in \mathbb{C}(X)$ dont 0 n'est pas pôle, alors $\tilde{F}$ est d.s.e. avec pour rayon de convergence le module minimum des pôles de F, càd de disque le plus grand ne contenant aucun pôle, de plus le développement est combinaison linéaire des $\sum_{n=0}^{\infty}\binom{n+k}{k}z^n = \frac{1}{(1-z)^{k+1}}$ k variant dans $\mathbb{N}$.

Une fraction rationnelle complexe est holomorphe au point ∞ de la sphère de Riemann ssi son degré est ≤ 0 ssi $degN \leq degD$.

Une fraction rationnelle complexe est méromorphe sur la sphère de Riemann.

V.2.3. Décomposition en éléments simples dans $\mathbb{R}$

Etant donne la forme d'un polynôme irréductible réel, on trouve deux types d'éléments simples $A_{i,j}$

Elément simple de première espèce $\frac{c}{X-\alpha}$, $c \in \mathbb{R}, \alpha \in \mathbb{R}$

Elément simple de seconde espèce $\frac{cX+d}{(X^2+pX+q)^n}$, $c, d, p, q \in \mathbb{R}, p^2 - 4q < 0$

On peut passer par la décomposition dans $\mathbb{C}$, et regrouper les pôles conjugués, mais en général on évite et on essaye d'appliquer les méthodes astucieuses.

V.3. Applications de la décomposition en éléments simples

V.3.1. Application en algèbre linéaire

Pour $A, B \in K[X]$ tels que $A \wedge B = 1$ on peut écrire la décomposition en éléments simples $\frac{1}{AB} = \frac{U}{B} + \frac{V}{A}$ pour trouver les coefficients de Bézout dans la formule $1 = AU + BV$.

Si $P(X) = \prod_{j=1}^{n}(X - \alpha_j)$ alors $\frac{P'(X)}{P(X)} = \sum_{j=1}^{n}\frac{1}{X-\alpha_j}$

V.3.2. Theoreme de Gauss-Lucas

Pour un polynôme complexe de degré $n \geq 2$, les racines du polynôme dérivé sont dans l'enveloppe convexe des racines du polynôme.

Si le polynôme est scindé dans $\mathbb{R}$, les racines complexes du polynôme dérivé sont donc en particulier toutes réelles, P' est scindé dans $\mathbb{R}$. On sait même qu'elles se trouvent entre les racines de P, par Rolle.

V.3.3. Application aux dénombrements

$\frac{1}{1-x^{a_j}} = \sum_{p=0}^{\infty} x^{pa_j}$

$F = \frac{1}{(1-x^{a_1})\dots(1-x^{a_n})} = \prod_{j=1}^{\infty} \sum_{p_j=0}^{\infty} x^{p_j a_j} = \sum_{(p_1,\dots,p_m)}^{\infty} x^{a_1 p_1 + \dots + a_m p_m} = \sum_{n=0}^{\infty} a(n) x^n$

La décomposition en éléments simples de F fait apparaitre des éléments simples de la forme $\frac{c}{(1-\zeta x)^k}$ ou ζ est une racine de l'unite d'ordre l'un des a_i, k est un entier, c est un nombre complexe. Chacun de ces éléments simples peut être développé en série entière de rayon 1. F peut donc ainsi s'exprimer comme série entière, ce qui donne tous les $a(n)$.

V.4. Déterminants de Hankel

Si $\sum_{n\geq 0} a_n x^n$ est une série entière à coeffs dans C, de rayon $R > 0$, on note $F(x)$ la somme pour $|x| < R$. Alors $F|D(0,R)$ fonction rationnelle ssi $\exists p, q \in N\ \forall n > p$ $\begin{vmatrix} a_n & a_{n+1} & \dots & a_{n+q} \\ a_{n+1} & a_{n+2} & \dots & a_{n+q+1} \\ \dots & \dots & \dots & \dots \\ a_{n+q} & \dots & \dots & a_{n+2q} \end{vmatrix} = 0$

Ces déterminants sont appelés **déterminants de Hankel**.

Complément 1. Application géométrique du résultant

1.1. Cas affine

1.2. Cas projectif

Recherche pratique des points d'intersection.

Complément 2. Sous-variétés algébriques de C^n et ideaux de $C[X_1, \dots, X_n]$

Complément 3. Polynômes cyclotomiques

Soit U l'ensemble des nombres complexes de module 1. C'est un groupe pour la multiplication.

L'indicatrice d'Euler est l'application $\phi: N^* \to N^*: n \mapsto card(\{k \in \{0, \dots, n-1\} \mid k \wedge n = 1\})$

Une racine nième de l'unité est un complexe z tel que $z^n = 1$.

Pour $n \in N^*$ les racines n-iemes de l'unité sont exactement les $\alpha_k = e^{\frac{2i\pi k}{n}},\ k \in \{0, \dots, n-1\}$

Les n racines n-iemes de l'unité forment un groupe cyclique d'ordre n : $\boldsymbol{U_n} \approx \frac{Z}{nZ}$ sous-groupe de $(U,\times)$

Une **racine primitive n-ieme de l'unité** est une racine nième de l'unité d'ordre n dans $(U_n,\times)$, autrement dit c'est un α_k avec $k \in \{0, \dots, n-1\}, k \wedge n = 1$. Il y en a donc $\phi(n)$ distinctes.

Formule d'Euler. $\forall n \in N^*\ n = \sum_{d|n} \phi(d)$

On note $\boldsymbol{U_n}'$ le groupe des racines primitives n-ieme de l'unité $U_n' \approx \left(\frac{Z}{nZ}\right)^{\times}, U_n' \subseteq U_n$

On a $U_n = \cup_{d|n} U_d'$ et les U_d' sont disjoints 2 a 2. Les $\{U_d' : d|n\}$ forment une partition de U_n

Le **n-ieme polynome cyclotomique est $\boldsymbol{\phi_n}(\boldsymbol{X}) = \prod_{\zeta \in U_n'}(X - \zeta) = \prod_{\substack{1\leq k\leq n \\ k\wedge n=1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$**

Les polynômes cyclotomiques sont unitaires.

$\forall n \in \mathbb{N}^*\ \deg(\phi_n) = \phi(n)$

Formule d'Euler cyclotomique. On a $X^n - 1 = \prod_{\alpha \in U_n}(X - \alpha) = \prod_{d|n} \phi_d(X)$

Pour p premier $\phi_p = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \dots + X^{p-1}$

Pour p premier $\phi_{p^2} = \frac{X^{p^2} - 1}{X^p - 1} = 1 + X^p + X^{2p} + \dots + X^{p(p-1)}$

Les polynômes cyclotomiques sont dans $\mathbb{Z}[X]$.

Pour $n \geq 2$, ϕ_n est un polynôme réciproque, càd que dans la suite de ses coefficients, le premier est égal au dernier, le deuxième à l'avant dernier, etc… càd $X^{\phi(n)} \phi_n\left(\frac{1}{X}\right) = \phi_n$.

Les polynômes cyclotomiques sont irréductibles dans $\mathbb{Q}[X]$.

Soit $\zeta \in U_n'$, on a $\phi_n(\zeta) = 0$, avec $\phi_n \in \mathbb{Q}[X]$, donc $I_\zeta^{\mathbb{Q}} \neq \{0\}$

$\mathbb{Q}(\zeta)$ est une extension algébrique simple de $\mathbb{Q}$ appelée ***n*-ième corps cyclotomique**.

Donc $\mathbb{Q}(\zeta) = \mathbb{Q}[\zeta] \approx \frac{\mathbb{Q}[X]}{\langle \pi_\zeta \rangle}$ et ce sont des corps.

En fait ϕ_n est le polynôme minimal sur $\mathbb{Q}$ de toute racine primitive de U_n. $\pi_\zeta = \phi_n$

Donc $\mathbb{Q}(\zeta) = \mathbb{Q}[\zeta] \approx \frac{\mathbb{Q}[X]}{\langle \phi_n(X) \rangle}$

$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \pi_\zeta = \phi(n)$

$\mathbb{Q}(\zeta)$ est un corps de rupture de ϕ_n sur $\mathbb{Q}$, car $\phi_n(\zeta) = 0$.

$\mathbb{Q}(\zeta)$ est en fait un corps de décomposition de ϕ_n sur $\mathbb{Q}$, donc $\mathbb{Q}(\zeta)$ est une extension galoisienne.

Si $n|m$, le n ième corps cyclotomique est un sous-corps du m ième.

Complément 4. Polynômes invariants sous le groupe alterné

4.1. Cas ou 2 est inversible dans A

4.2. Cas général

Complément 5. Groupe des K automorphismes de $K[X]$

Résumé des propriétés de structure. TODO

Pour K corps, $K[X]$ anneau intègre, principal, euclidien, noethérien, factoriel, de Bézout, à pgcd.

Pour K corps, $K[X_1, \dots, X_n]$ anneau intègre, noethérien, pas principal donc pas euclidien.

Dans un anneau commutatif A, $A[X]$ anneau principal ssi A corps.

$Z[i]$ est un anneau euclidien, donc principal.

$Z[X]$ non principal, donc non euclidien

$\frac{Z[T]}{T^2+5}$ est un anneau intègre, noethérien mais pas factoriel.

Si A anneau commutatif noethérien, alors $A[X]$ noethérien.

Si A anneau factoriel, $A[X]$ anneau factoriel.

Si A anneau factoriel, alors $A[X_1, \dots, X_n]$ anneau factoriel.

Même si A est un corps, $A[(X_n)_{n\in\mathbb{N}}]$ n'est jamais noethérien.

Exercices.

Sur $K[X]$, avec $a, b \in \mathbb{N}^*$, $X^a - 1 \wedge X^b - 1 = X^{a\wedge b} - 1$

Un corps fini n'est jamais algébriquement clos car $1 + \prod_{\alpha\in\mathbb{K}}(X - \alpha)$ n'a pas de racine sur $\mathbb{K}$.

Pour $n \geq 2$, $1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$ n'a que des racines simples dans $\mathbb{C}$.

Pour $n \geq 2$, $X^n - X + 1$ n'a que des racines simples dans $\mathbb{C}$.

Un polynôme de $\mathbb{Q}[X]$ irréductible sur $\mathbb{Q}[X]$, n'a que des racines simples dans $\mathbb{C}$.

Une racine d'ordre $>$ a la moitié du degré d'un polynôme de $\mathbb{Q}[X]$, est rationnelle $\lambda \in \mathbb{Q}$.

$P \in \mathbb{Q}[X], \deg P = 2n + 1, n \geq 2, P$ admet une racine d'ordre n, alors P admet une racine dans $\mathbb{Q}$.

$\forall P \in \mathbb{C}[X]$ $P(X^2) = P(X)P(X + 1) \Leftrightarrow \exists p \in \mathbb{N}^*$ $P = X^p(X - 1)^p$

Pour $x_1, \dots, x_p$ distincts dans un corps, $n_1, \dots, n_p \in \mathbb{N}, n \in \mathbb{N}$, alors $\exists P \in \mathbb{K}[X], \deg P < n, \forall i \in [\![1, p]\!]\ \forall k \in [\![0, n_i - 1]\!]\ P^{(k)}(x_i) = y_{i,k}$ avec $y_{i,k} \in \mathbb{K}$ fixés. De plus pour $f \in C^n(I, \mathbb{R})$ on a alors $\forall x \in I\ \exists \xi \in I\ f(x) = P(x) + \frac{f^{(n)}(\xi)}{n!}\prod_{i=1}^{p}(x - x_i)^{n_i}$

$\forall P = \lambda \prod_{i=1}^{n}(X-\alpha_i)^{m_i} \in \mathbb{R}[X]$ scindé sur $\mathbb{R}$, de degré $n \geq 2$, alors $\forall i \in [\![1, n-1]\!]$ $P'\left(\frac{a_i+a_{i+1}}{2}\right) = 0$ ssi $n = \deg P = 2$.

Principe du maximum. Un polynôme complexe non constant P vérifie $\forall r \in \mathbb{R}_+^*$ $\forall z_0 \in D(0,r)$ $|P(z_0)| < \sup_{|z|=r}|P(z)|$. Plus généralement $\forall C$ compact $\subseteq \mathbb{C}$ $\forall z_0 \in Int(C)$ $|P(z_0)| < \sup_{|z|\in Fr(C)}|P(z)|$

Pour $a_1, \dots, a_n \in \mathbb{N}$ distincts, $(\prod_{k=1}^{n}(X-a_k)) - 1$ est irréductible dans $\mathbb{Z}[X]$

Pour $a_1, \dots, a_n \in \mathbb{N}$ distincts, $(\prod_{k=1}^{n}(X-a_k)^2) + 1$ est irréductible dans $\mathbb{Z}[X]$

Pour $a_1, \dots, a_n \in \mathbb{N}$ distincts, $(\prod_{k=1}^{n}(X-a_k)^4) + 1$ est irréductible dans $\mathbb{Z}[X]$

Polynômes de Tchebychev. $\forall n \in \mathbb{N}^*$ $\exists ! \boldsymbol{T_n} \in \mathbb{R}[X]$ $\forall \theta \in \mathbb{R}$ $T_n(\cos(\theta)) = \cos(n\theta)$

On a $T_n(x) = \sum_{k=0}^{E\left(\frac{n}{2}\right)}\binom{n}{2k}x^{n-2k}(x^2-1)^k$, donc le coeff dominant est $\sum_{k=0}^{E\left(\frac{n}{2}\right)}\binom{n}{2k} = 2^{n-1}$

Un polynôme réel unitaire de degré n verifie $\|P\|_{u,[-1,1]} \geq 2^{1-n}$

Pour $F \in \mathbb{C}(X)$ non constante, soit $F(D_F) = \mathbb{C}$, soit $F(D_F) = \mathbb{C} \setminus \{\alpha\}$ avec $F = \alpha + \frac{1}{P}$ avec $P \in \mathbb{C}[X]$ non constant.

Pour $F, G \in \mathbb{C}(X)$, $F \circ G$ est défini ssi G n'est pas une constante qui est un pôle de F.

Pour $F, G \in \mathbb{C}(X)$, $F \circ G$ est un polynôme ssi 1), 2), 3), ou 4)

1) F est constant.

2) G est constant et pas un pôle de F.

3) F et G sont des polynômes.

4) $F = \frac{P}{(X-\alpha)^h}$ avec $P \in \mathbb{C}[X], \deg P \leq h$, et $G = \alpha + \frac{1}{Q}$ avec $Q \in \mathbb{C}[X]$

La transformée de Fourier discrète d'un polynôme est $F_d(P) = \sum_{k=0}^{n-1} P\left(e^{\frac{2ik\pi}{n}}\right)X^k$, en posant $\overline{F_d}(P) = \sum_{k=0}^{n-1} P\left(e^{\frac{-2ik\pi}{n}}\right)X^k$, alors formule d'inversion : $\overline{F_d}\left(F_d(P)\right) = nP$

Un polynôme $P \in \mathbb{Z}[X]$ tel que $\forall j \in \mathbb{Z}$ $\left|P\left(e^{\frac{2ik\pi}{n}}\right)\right| \leq 1$ et $\exists k \in \{0,1,\dots,n-1\}$ $P\left(e^{\frac{2ik\pi}{n}}\right) = 0$, est divisible par $X^n - 1$.

Pour $P \in \mathbb{C}[X]$ tel que $\forall n \in \mathbb{N}$ $P(n) \in \mathbb{Z}$, alors $P \in \mathbb{Q}[X]$ et $(\deg P\,!)P \in \mathbb{Z}[X]$

Une fraction rationnelle complexe dont l'image de tout naturel non pole est dans $\mathbb{Q}$, est dans $\mathbb{Q}(X)$

Une fraction rationnelle complexe dont l'image de tout naturel non pole est dans $\mathbb{Z}$, est dans $\mathbb{Q}[X]$

L'ensemble des réels algébriques sur $\mathbb{Q}$ est dénombrable. Donc il existe des réels transcendants.