Chapitre 3

Anneaux de polynômes

3.1 Critères d'irréductibilité

Définition 3.1.1. Soit A un anneau commutatif intègre. Un polynôme $P \in A[X]$ est primitif si et seulement si 1 est PGCD de ses coefficients (les coefficients sont premiers entre eux dans leur ensemble).

On note $\mathcal{Q}(A)$ le corps des fractions de A. L'anneau $A[X]$ est (isomorphe à) un sous-anneau de $\mathcal{Q}(A)[X]$

Proposition 3.1.2. *Soit $P \in A[X]$ un polynôme non constant (de degré supérieur ou égal à 1).*

1. *Si P est irréductible dans $A[X]$, alors il est primitif.*
2. *Si P est primitif et irréductible dans $\mathcal{Q}(A)[X]$, alors il est irréductible dans $A[X]$.*

Remarque 3.1.3. L'élément X de $A[X]$ est irréductible.

Réduction des coefficients

Soit I un idéal dans l'anneau commutatif A. La surjection canonique $\pi : A \to A/I$ s'étend en un morphisme d'anneau :

$$\begin{array}{rccc} \Pi : & A[X] & \to & A/I[X] \\ & P = \sum_k a_k X^k & \mapsto & \sum_k \overline{a}_k X^k \end{array} ,$$

et induit un isomorphisme : $A[X]/I \approx A/I[X]$.
L'image $\Pi(P)$ est appelée la réduction de P modulo I. Le coefficient dominant d'un polynôme P est le coefficient de plus haut degré.

Proposition 3.1.4. *Soit $P \in A[X]$ un polynôme primitif non constant, et I un idéal premier qui ne contient pas le coefficient dominant de P. Si la réduction de P modulo I est irréductible dans $A/I[X]$, alors P est irréductible dans $A[X]$.*

3.2 Factorialité des anneaux de polynômes

Définition 3.2.1. Soit A un anneau factoriel. On appelle contenu de $P \in A[X]$ un PGCD de ses coefficients. Il existe et est unique aux inversibles près.

On notera $c(P)$ le contenu de P : une classe d'éléments associés ou un représentant.

Remarque 3.2.2. Un polynôme est primitif si et seulement si son contenu est inversible.

Proposition 3.2.3. *Pour P et Q dans $A[X]$, avec A factoriel, on a $c(PQ) = c(P)c(Q)$. En particulier le produit de deux polynômes primitifs est primitif.*

Lemme 3.2.4. *Soient $P \in A[X]$ un polynôme non constant primitif qui s'écrit $P = QR$ dans $\mathcal{Q}(A)[X]$, alors il existe $\lambda \in \mathcal{Q}(A)^\times$ tel que : $P = Q_1R_1$ dans $A[X]$, avec $P_1 = \lambda P$, $Q_1 = \frac{1}{\lambda}Q$.*

Fin du cours du 5 octobre

Lemme 3.2.5. *Si $P \in A[X]$ est divisible dans $\mathcal{Q}(A)[X]$ par un polynôme primitif $Q \in A[X]$, alors P est divisible par Q dans $A[X]$.*

Théorème 3.2.6. *Soit A un anneau factoriel. Alors :*
a) les polynômes constants irréductibles dans $A[X]$ sont les irréductibles de A ;
b) les polynômes non constants irréductibles dans $A[X]$ sont les polynômes non constants primitifs de $A[X]$ qui sont irréductibles dans $\mathcal{Q}(A)[X]$.
c) l'anneau $A[X]$ est factoriel.

Proposition 3.2.7 (Critère d'Eisenstein)**.** *Soient A un anneau factoriel, f un élément irréductible de A, et*

$$P = \sum_{k=0}^{n} a_k X^k$$

un polynôme non constant primitif dans $A[X]$.
Si : $f \not| a_n$, $\forall i < n$ $f | a_i$, et $f^2 \not| a_0$, alors P est irréductible dans $A[X]$.

3.3 Polynômes en une variable : compléments

3.3.1 La division euclidienne étendue

Théorème 3.3.1. *Soient $U = a_n X^n + \cdots + a_0$ et $V = b_m X^m + \cdots + b_0$ deux polynômes dans $A[X]$, avec $n \geq m-1$ et $b_m \neq 0$. Il existe un unique couple (Q, R) de polynômes de $A[X]$, tels que :*

$$b_m^{n-m+1} U = VQ + R \ , \ et \quad (\ R = 0 \ ou \ \deg(R) < \deg(Q) \ ) \ .$$

3.3.2 Fonctions polynomiales et évaluation

L'évaluation permet de définir un morphisme d'anneau :

$$\begin{array}{rccc} E: & A[X] & \to & \mathcal{A}(A, A) \\ & P & \mapsto & [a \mapsto P(a)] \end{array}$$

L'image de ce morphisme est le sous anneau des fonctions polynomiales sur A.

Proposition 3.3.2. *a) Si A est infini, alors E est injective.*
b) Si A est un corps fini à q éléments, alors le noyau de E est l'idéal engendré par $X^q - X$.

Fin du cours du 9 octobre

3.3.3 Dérivation

Caractéristique d'un anneau

Si A est un anneau commutatif, alors il existe un unique morphisme d'anneau $\eta : \mathbb{Z} \to A$.

Définition 3.3.3. La caractéristique d'un anneau A est le générateur (entier positif ou nul) de l'idéal $\mathrm{Ker}(\eta)$.

Remarque 3.3.4. L'image de η est isomorphe à $\mathbb{Z}/\mathrm{Ker}(\eta)$. Pour un anneau intègre, c'est un sous-anneau intègre. La caractéristique d'un anneau intègre est soit zéro, soit un nombre premier.

Définition 3.3.5. Soit A un anneau commutatif intègre de caractéristique $p > 0$, alors l'application

$$\begin{array}{rccc} F: & A & \to & A \\ & a & \mapsto & a^p \end{array}$$

est un morphisme d'anneau.

Dérivation

La dérivation est l'application :

$$\begin{array}{rccc} D: & A[X] & \to & A[X] \\ & P=\sum_k a_k X^k & \mapsto & D.P=P'=\sum_{k>0} a_k k X^{k-1} \end{array}$$

Théorème 3.3.6. *Soit A un anneau intègre, et $P \in A[X]$.*

1. *Si la caractéristique de A est nulle, on a :*

$$DP = 0 \Leftrightarrow P = 0 \ .$$

2. *Si la caractéristique de A est un nombre non nul p (premier), alors :*

$$DP = 0 \Leftrightarrow P \in A[X^p] \ .$$

Théorème 3.3.7 (Formule de Taylor)**.** *Soit A un anneau commutatif intègre de caractéristique nulle, pour tout $P \in A[X]$, $D^k.P(0)$ est divisible par $k!$, et :*

$$P = \sum_k \frac{D^k P(0)}{k!} X^k \ .$$

3.4 Polynômes à n variables

Soit A un anneau commutatif et $X_1, \ldots, X_n$ des *indéterminées*. On note $A[X_1, \ldots, X_n]$ l'ensemble des familles d'éléments de A indexées par $\mathbb{N}^n$, avec un nombre fini de termes non nuls, notées comme combinaisons linéaires des $X_1^{k_1} \ldots X_n^{k_n}$, $k_j \geq 0$: les éléments de $A[X_1, \ldots, X_n]$ s'écrivent sous la forme :

$$P = \sum_{k_1,\ldots,k_n} a_{k_1,\ldots,k_n} X_1^{k_1} \ldots X_n^{k_n} = \sum_{\underline{k}} a_{\underline{k}} X_1^{k_1} \ldots X_n^{k_n} \ .$$

$A[X_1, \ldots, X_n]$ est muni des opérations :

$$(\sum_{\underline{k}} a_{\underline{k}} X_1^{k_1} \ldots X_n^{k_n}) + (\sum_{\underline{k}} b_{\underline{k}} X_1^{k_1} \ldots X_n^{k_n}) = \sum_{\underline{k}} (a_{\underline{k}} + b_{\underline{k}}) X_1^{k_1} \ldots X_n^{k_n}.$$

$$(\sum_{\underline{k}} a_{\underline{k}} X_1^{k_1} \ldots X_n^{k_n})(\sum_{\underline{l}} b_{\underline{l}} X_1^{l_1} \ldots X_n^{l_n}) = \sum_{\underline{\nu}} c_{\underline{\nu}} X_1^{\nu_1} \ldots X_n^{\nu_n} \ ,$$

$$\text{avec } c_{\underline{\nu}} = \sum \underline{k} + \underline{l} = \underline{\nu} a_{\underline{k}\underline{b}_{\underline{l}}} \ ,$$

et de l'application de structure :

$$\begin{array}{rccc} \eta: & A & \to & A[X_1, \ldots, X_n] \\ & a & \mapsto & aX^0 = a \end{array}$$

Proposition 3.4.1. *$A[X_1, \ldots, X_n]$ est une algèbre sur A.*

Remarque 3.4.2. L'application qui définit la structure d'algèbre est injective, d'image les polynômes constants ; A est identifié au sous-anneau de $A[X_1, \ldots, X_n]$ formé par les polynômes *constants*.

Proposition 3.4.3 (Propriété universelle)**.** *Soit B une algèbre sur l'anneau commutatif A, et $b_1, \ldots, b_n$ des éléments de B, alors il existe un unique morphisme d'algèbre $E_{(b_1,\ldots,b_n)} : A[X_1, \ldots, X_n] \to B$ qui envoie chaque X_i sur b_i.*

Proposition 3.4.4. *Les anneaux $A[X_1, \ldots, X_{n-1}, X_n]$ et $A[X_1, \ldots, X_{n-1}][X_n]$ sont isomorphes.*

Corollaire 3.4.5. *Si l'anneau A est factoriel, alors $A[X_1, \ldots, X_n]$ est factoriel.*

Définition 3.4.6. Le multidegré d'un monôme $a_{k_1,\ldots,k_n} X_1^{k_1} \ldots X_n^{k_n}$ est la suite des exposants $(k_1, \ldots, k_n)$; son degré total ou simplement son degré est la somme des exposants : $|\underline{k}| = \sum_i k_i$.
Le degré d'un polynôme non nul est le maximum des degrés (totaux) de ses monômes.
Un polynôme est homogène si et seulement si tous ses monômes ont même degré (total).

Dérivées partielles

On définit les dérivées partielles avec les formules habituelles ; on note $D_j = \frac{\partial}{\partial X_j}$ la dérivation par rapport à la variable X_j.

Remarque 3.4.7. Le lemme de Schwarz $D_i \circ D_j = D_j \circ D_i$ est immédiat pour les polynômes.

Théorème 3.4.8 (Formule de Taylor)**.** *Soient A un anneau commutatif intègre de caractéristique 0, et $P \in A[X_1, \ldots, X_n]$. On a :*

$$P = \sum_{\underline{k}} \frac{1}{k_1! \ldots k_n!} \frac{\partial^{|\underline{k}|P}}{\partial X_1^{k_1} \ldots \partial X_n^{k_n}} (0, \ldots, 0) X_1^{k_1} \ldots X_n^{k_n} \ .$$

Proposition 3.4.9. *Soit $P \in A[X_1, \ldots, X_n]$ un polynôme homogène de degré d, alors :*

$$\sum_i X_i \frac{\partial P}{\partial X_i} = dP \ .$$

3.5 Polynômes symétriques

Le groupe symétrique $\mathcal{S}_n$ agit à gauche sur $A[X_1, \ldots, X_n]$ par permutation des variables : pour $\sigma \in \mathcal{S}_n$,

$$\sigma.P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \ .$$

Définition 3.5.1. Les polynômes invariants sous l'action du groupe symétrique forme un sous-anneau de $A[X_1, \ldots, X_n]$: le sous-anneau des polynômes symétriques, noté $A[X_1, \ldots, X_n]^{sym}$.

Polynômes symétriques élémentaires

Définition 3.5.2. Pour $1 \leq k \leq n$ le polynôme symétrique élémentaire $\sigma_k \in A[X_1, \ldots, X_n]^{sym}$ est le coefficient de degré $n-k$ du polynôme :

$$\prod_i (T + X_i) \in A[X_1, \ldots, X_n][T] \ .$$

Remarques 3.5.3. 1. On a : $\sigma_k = \sum_{i_1 < i_2 < \cdots < i_k} X_{i_1} \ldots X_{i_k}$.

2. Relations entre coefficients et racines :

$$\prod_{i=1}^{n} (X - \alpha_i) = X^n + \sum_{k=1}^{n} (-1)^k \sigma_k(a_1, \ldots, a_n) X^{n-k} \ .$$

Théorème 3.5.4. *Tout polynôme symétrique s'écrit de manière unique comme un polynôme dans les polynômes symétriques élémentaires : le morphisme d'algèbre de $A[Y_1, \ldots, Y_n]$ dans $A[X_1, \ldots, X_n]^{sym}$ qui envoit Y_k sur σ_k est un isorphisme d'algèbre.*

Fin du cours du 12 octobre

Polynômes antisymétriques

Définition 3.5.5. Un polynôme $P \in A[X_1, \ldots, X_n]$, avec A anneau commutatif intègre de caractéristique différente de 2, est antisymétrique si et seulement si :

$$\forall \sigma \in \mathcal{S}_n \ , \ \sigma.P = \epsilon_\sigma P \ ,$$

où ϵ_σ est la signature.

Remarque 3.5.6. Il suffit de vérifier la condition pour les transpositions.

Exercice 3.5.7. Soit A un anneau commutatif intègre de caractéristique différente de 2. Montrer qu'un polynôme $P \in A[X_1, \ldots, X_n]$ est anti-symétrique si et seulement s'il s'écrit sous la forme :

$$P = \Delta_n Q \ , \quad \text{avec } \Delta_n = \prod_{i<j}(X_j - X_i) \ \text{ et } Q \in A[X_1, \ldots, X_n]^{sym} \ .$$

Remarque. Δ_n est le déterminant de Vandermonde :

$$\Delta_n = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_n \\ \vdots & \vdots & \ldots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \ldots & X_n^{n-1} \end{vmatrix} .$$

3.6 Résultant et discriminant

Le déterminant d'une matrice carrée d'ordre n à coefficients dans un anneau commutatif, est défini par la formule habituelle :

$$\det A = \sum_{\sigma \in \mathcal{S}_n} \epsilon_\sigma \prod_{i=1}^{n} a_{i\sigma(i)} \ .$$

Notons que cela a un sens si les n^2 coefficients de la matrice sont des variables différentes : on peut voir le déterminant comme un polynôme en n^2 variables.

Définition 3.6.1. Soient $P = a_0 + \cdots + a_m X^m$ et $Q = b_0 + \cdots + b_n X^n$ deux polynômes à coefficients dans un anneau commutatif. Le résultant $\mathrm{Res}(P, Q)$ est le déterminant de la matrice dite de Sylvester :

$$\mathcal{S}(a_0, \ldots, a_m; b_0, \ldots, b_n) = \begin{pmatrix} a_0 & & & & b_0 & & & & \\ a_1 & a_0 & & & b_1 & b_0 & & & \\ \vdots & a_1 & \ddots & & \vdots & b_1 & \ddots & & \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & \ddots & \\ \vdots & \vdots & & a_1 & b_n & \vdots & & \ddots & b_0 \\ a_m & \vdots & & \vdots & & b_n & & & b_1 \\ & a_m & & & & & \ddots & & \\ & & \ddots & \vdots & & & & \ddots & \vdots \\ & & & a_m & & & & & b_n \end{pmatrix}$$

Proposition 3.6.2. *Dans le cas d'un corps commutatif* $\mathbb{K}$ *:*
a) $\mathrm{Res}(P,Q)$ *est le déterminant de l'application :*

$$\begin{array}{rccc} \Phi: & \mathbb{K}_n[X]\times\mathbb{K}_m[X] & \to & \mathbb{K}_{n+m}[X] \\ & (U,V) & \mapsto & UP+VQ \end{array}$$

dans les bases $(1,X,\dots,X^{n-1},1,\dots,X^{m-1})$ *et* $(1,X,\dots,X^{m+n-1})$.
b)

$$\mathrm{Res}(P,Q)=b_n^{\deg(P)}\det(\psi_P)\ ,$$

où b_n *est le coefficient dominant de* Q*, et :*

$$\begin{array}{rccc} \psi_P: & \mathbb{K}[X]/(Q) & \to & \mathbb{K}[X]/(Q) \\ & \overline{U} & \mapsto & \overline{UP} \end{array}$$

Fin du cours du 16 octobre

Théorème 3.6.3. *Dans le cas d'un corps commutatif* $\mathbb{K}$*, le résultant de* P *et* Q *est non nul si et seulement si* P *et* Q *sont premiers entre eux.*

Proposition 3.6.4. *a)* $\mathrm{Res}(P,Q)=(-1)^{nm}\mathrm{Res}(Q,P)$.
b) $\mathrm{Res}(P_1P_2,Q)=\mathrm{Res}(P_1,Q)\mathrm{Res}(P_2,Q)$.
c) Si le polynôme Q *est scindé :* $Q=b_n\prod_{j=1}^{n}(X-y_j)$*, alors :*

$$\mathrm{Res}(P,Q)=b_n^{\deg(P)}\prod_{i=1}^{m}P(y_j)\ .$$

d) Si P *est également scindé :* $P=a_m\prod_{i=1}^{m}(X-x_i)$*, alors :*

$$\mathrm{Res}(P,Q)=a_m^n b_n^m\prod_{i=1}^{m}\prod_{j=1}^{n}(y_j-x_i)\ .$$

Discriminant

Soit $P=a_0+\cdots+a_nX^n$ un polynôme de degré n à coefficients dans un anneau commutatif intègre A.

Définition 3.6.5. Le discriminant de P, noté $\mathrm{Disc}(P)$ est défini par :

$$\mathrm{Disc}(P) = (-1)^{\frac{n(n-1)}{2}} \begin{vmatrix} a_0 & & & & a_1 & & & & \\ a_1 & a_0 & & & 2a_2 & a_1 & & & \\ \vdots & a_1 & \ddots & & \vdots & 2a_2 & \ddots & & \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & \ddots & \\ \vdots & \vdots & & a_1 & na_n & \vdots & & \ddots & a_1 \\ a_n & \vdots & & \vdots & & na_n & & & 2a_2 \\ & \ddots & & & & & \ddots & & \\ & & a_n & a_{n-1} & & & & na_n & (n-1)a_{n-1} \\ & & & 1 & & & & & n \end{vmatrix}$$

Lorsque na_n est non nul : $a_n \mathrm{Disc}(P) = (-1)^{\frac{n(n-1)}{2}} \mathrm{Res}(P, P')$.

Théorème 3.6.6. *Si le polynôme P, à coefficients dans le corps commutatif $\mathbb{K}$, est scindé : $P = a_n \prod_{i=1}^{n} (X - x_i)$, alors :*

$$\mathrm{Disc}(P) = a_n^{2n-2} \prod_{i<j} (x_j - x_i)^2 \ .$$

Le discriminant générique est le carré du déterminant de Vandermonde :

$$\Delta_n^2 = \prod_{1 \le i < j \le n} (X_j - X_i)^2$$

C'est un polynôme symétrique.

Proposition 3.6.7. *On a :*

$$\Delta_n^2 = \begin{vmatrix} n & p_1 & p_2 & \dots & p_{n-1} \\ p_1 & p_2 & p_3 & \dots & p_n \\ p_2 & p_3 & p_4 & \dots & p_{n+1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \dots & p_{2n-2} \end{vmatrix} ,$$

où $p_k = \sum_i X_i^k$ est la somme des puissances.