P. Maurer

ENS Rennes

Recasages : 122, 141, 142.

Référence : Perrin, Cours d'Algèbre & FGN, Oraux X-ENS, Algèbre 1

Critère d'Eisenstein

A désigne un anneau factoriel, et K désigne son corps des fractions.

Definition 1. *$P \in A[X]$ est dit irréductible si il n'est ni inversible ni produit de deux polynômes non inversibles dans $A[X]$.*

Definition 2. *Si $P \in A[X]$, on appelle contenu de P et on note $c(P)$ le plus grand diviseur commun de ses coefficients, défini à un inversible près. P est dit primitif si $c(P) = 1$.*

Lemma 3. *(Gauss)*

Soit $P, Q \in A[X]$. Alors $c(PQ) = c(P)\,c(Q)$.

Theorem 4. *Soit $P \in A[X]$. Alors P est irréductible dans $A[X]$ si et seulement si P est irréductible dans $K[X]$ et primitif.*

Proof.

$\boxed{\Longrightarrow}$ Par définition du contenu, on peut écrire $P = c(P) \cdot \tilde{P}$. Comme P est irréductible, $c(P)$ est nécessairement inversible, d'où $c(P) = 1$ (à inversible près).

Soit $Q, R \in K[X]$ tels que $P = QR$. Il existe $r \in A$ et $q \in A$ tels que rR et qQ soient dans $A[X]$ et primitifs. On a alors $qr\,P = (rR)\,(qQ)$, donc d'après le lemme de Gauss, $qr = c(rR)\,c(qQ) = 1$. Donc q et r sont des inversibles de $A[X]$, d'où $R \in A[X]$ et $Q \in A[X]$: comme P est irréductible, Q est un inversible dans $A[X]$ ou R est un inversible dans $A[X]$, donc Q est un inversible dans $K[X]$ ou R est un inversible dans $K[X]$. Ainsi, P est irréductible dans $K[X]$.

$\boxed{\Longleftarrow}$ Soit $P \in A[X]$, primitif et irréductible dans $K[X]$. Soit $Q, R \in A[X]$ tels que $P = QR$. Comme $Q \in K[X]$ et $R \in K[X]$, on en déduit que l'un des deux, disons Q, est un élément de $K^{\times}$. On a alors, en passant au contenu : $c(P) = c(Q)\,c(R) = Q\,c(R)$.

D'après le lemme de Gauss, $1 = Q\,c(R)$, avec $c(R) \in A$: on en déduit que $Q \in A^{\times}$. Donc P est irréductible dans $A[X]$. □

Theorem 5. *(Critère d'Eisenstein)*

Soit $P = \displaystyle\sum_{i=1}^{n} a_i X^i \in A[X]$, avec $n \geq 1$. On suppose qu'il existe $p \in A$ irréductible tel que :

- *p divise a_i pour tout $i \in [\![0, n-1]\!]$.*
- *p ne divise pas a_n.*
- *p^2 ne divise pas a_0.*

Alors P est irréductible dans $K[X]$.

Proof. Supposons par l'absurde que P n'est pas irréductible dans $K[X]$. D'après le théorème précédent, P n'est pas non plus irréductible dans $A[X]$. Le degré de P étant au moins 1, $P \notin A^{\times}$, donc il existe $Q, R \in A[X]$ non inversibles tels que $P = QR$.

Ecrivons $Q = \sum_{i=0}^{q} b_i X^i$ et $R = \sum_{i=0}^{r} c_i X^i$, avec $r + q = \deg(P)$, et $b_i, c_i \in A$. Comme p est irréductible, l'idéal engendré par p est premier, donc $B = A/(p)$ est intègre. On projette l'égalité $P = QR$ dans $B[X]$, en désignant par $\pi: A \to B$ la projection canonique. On a alors :

$$\pi(P) = \pi(a_n)\, X^n = (\pi(b_q) X^q + \cdots + \pi(b_0))(\pi(c_r) X^r + \cdots + \pi(c_0))$$

Comme $a_0 = b_0\, c_0$, on a $\pi(a_0) = \pi(b_0)\, \pi\,(c_0) = 0$. Comme B est intègre et que p^2 ne divise pas a_0, on a soit $\pi(b_0) = 0$ et $\pi(c_0) \neq 0$, soit $\pi(b_0) \neq 0$ et $\pi(c_0) = 0$. Par symétrie, on peut supposer qu'on est dans le premier cas.

On a alors $\pi(Q) \neq 0$, donc il existe $i \in [\![0, r-1]\!]$ tel que $\pi(b_{i+1}) \neq 0$, et $\pi(b_j) = 0$ pour tout $j \leq i$.

On a alors, par intégrité de B : $\pi(a_{i+1}) = \sum_{k=0}^{i+1} \pi(b_k)\, \pi(c_{i+1-k}) = \pi(b_{i+1})\, \pi(c_0) \neq 0$, mais $i + 1 \leq r < n$, contradiction puisque p divise a_{i+1}. □

Références

D. Perrin, *Cours d'Algèbre*.

FGN, *Algèbre 1*.