Critère d'Eisenstein

Leçons : 122, 125, 141

Réf. : Perrin, Cours d'algèbre p 51 et p 76

Lemme : (Gauss)

Soit A un anneau factoriel, $P, Q \in A[X]$.

Alors, $c(PQ) = c(P)\,c(Q)$ modulo $A^\times$

Prop. :

Soit A un anneau factoriel. Les polynômes de $A[X]$ irréductibles dans $A[X]$ sont :

1) les constantes $p \in A$, irréductibles dans A

2) les polynômes $P \in A[X]$ t.q. $\deg P \geq 1$, $c(P) = 1$ et irréductibles dans $K[X]$ où $K = Fr(A)$

Th. : (critère d'Eisenstein)

Soit A un anneau euclidien et $P = a_n X^n + \dots + a_0 \in A[X]$.

Soit $p \in A$ un élément irréductible de A.

Si : 1) $p \nmid a_n$

2) $\forall\, 0 \leq i \leq n-1$, $p \mid a_i$

3) $p^2 \nmid a_0$

Alors P est irréductible dans $K[X]$ (donc dans $A[X]$ si $c(P) = 1$)

Lemme :

1) Cas $c(P) = c(Q) = 1$

Par l'absurde, osp $c(PQ) \neq 1$. $P = a_n X^n + \dots + a_0$ et $Q = b_q X^q + \dots + b_0$

Soit $p \in A$ irréd., $p \mid c(PQ)$ (A est factoriel...)

$\exists\, 0 \leq i_0 \leq n$, $\forall\, 0 \leq i < i_0$, $p \mid a_i$ et $p \nmid a_{i_0}$ (car $c(P) = 1$)

$\exists\, 0 \leq j_0 \leq q$, $\forall\, 0 \leq j < j_0$, $p \mid b_{j_0}$ et $p \nmid b_{j_0}$ (car $c(Q) = 1$)

$p \mid c(PQ)$, donc en écrivant $PQ = \sum_{k=0}^{n+q} c_k X^k$,

$$p \mid c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j$$

donc $p \mid a_{i_0} b_{j_0}$ donc par le lemme d'Euclide, $p \mid a_{i_0}$ ou $p \mid b_{j_0}$ (absurde)

donc $\boxed{c(PQ) = 1}$

2) Cas général

Soit $d = c(P)$ et $e = c(Q)$.

On a alors $P = dP'$ où $c(P') = 1$ et $Q = eQ'$ où $c(Q') = 1$

donc $c(PQ) = c(deP'Q') = de\, c(P'Q') = de \times 1$

donc $\boxed{c(PQ) = c(P)c(Q)}$

n'est vrai que parce que $c(P'Q') = 1$ ($pgcd(2,4) \neq 8$)

Proposition :

1) Pq les polynômes cités sont bien irréductibles

a/ Soit $p \in A$, p irréductible dans A.

Si $p = QR$ où $Q, R \in A[X]$.

A est intègre donc $\deg Q = \deg R = 0$

donc $Q, R \in A$

donc $Q \in A^\times = A[X]^\times$ ou $R \in A^\times = A[X]^\times$

donc $\boxed{p \text{ est irréductible dans } A[X]}$

b/ Soit $P \in A[X]$, $c(P) = 1$ et P irréductible dans $K[X]$.

Si $P = QR$ dans $A[X]$, donc dans $K[X]$, comme P est irréductible dans $K[X]$, on a (par exemple) $Q \in K[X]^\times = K^\times$.

Donc, $\deg(Q) = 0$ donc $Q = a \in A$.

$P = aR$ donc $a \mid c(P) = 1$ donc $Q = a \in A^\times$

donc $\boxed{P \text{ est irréductible dans } A[X]}$

2) Mq ce sont les seuls irréductibles dans $A[X]$

Soit $P \in A[X]$ irréductible dans $A[X]$.

a°/ si $\deg P = 0$, alors $P = p \in A$ est nécessairement irréductible dans A

b°/ si $\deg P > 0$

On a nécessairement $c(P) = 1$.

Sinon, si $c(P) \neq 1$, $P = aP'$

- $a \notin A^\times = A[X]^\times$
- $\deg P' = \deg P > 0$ donc $P' \notin A^\times = A[X]^\times$

Mq P irréductible dans $K[X]$

Si $P = QR$ dans $K[X]$.

$\exists (a,b) \in A^2$, $a \wedge b = 1$ tels que $Q = \frac{a}{b} Q'$ où $\begin{cases} Q' \in A[X] \\ c(Q') = 1 \end{cases}$

$\exists (c,d) \in A^2$, $c \wedge d = 1$ ——— $R = \frac{c}{d} R'$ ——— $\begin{cases} c(R') = 1 \\ R' \in A[X] \end{cases}$

(si $Q = \sum_{i=0}^{k} \frac{a_i}{b_i} X^i$, $a = pgcd(a_i)$, $b = ppcm(b_i)$ puis on simplifie $\frac{a}{b}$)

On a alors $bd\,P = ac\,Q'R'$

donc par le lemme de Gauss

$c(bdP) = bd = c(ac\,Q'R') = ac$ modulo $A^\times$

donc $\lambda = \frac{ac}{bd} \in A^\times$

donc $P = \lambda Q'R'$ dans $A[X]$

On P est irréductible dans $A[X]$, donc Q' (ou R') $\in A[X]^\times = A^\times$

Donc $\deg Q' = \deg Q = 0$.

donc $Q \in K^\times = K[X]^\times$

donc P est irréductible dans $K[X]$

Critère d'Eisenstein

OPS $n = \deg P \geq 2$ (car si $\deg P = 0$ ou $\deg P = 1$, P est inductible dans $K[X]$)

On suppose P n'est pas inductible dans $K[X]$

P n'est alors pas inductible dans $A[X]$, et on peut écrire

(*) $P = QR$ où : . $Q, R \in A[X]$

. $\deg P > \deg Q$, $\deg R \geq 1$ (sinon P serait inductible dans $K[X]$)

Posons : . $Q = b_q X^q + \dots + b_0$, $R = c_r X^r + \dots + c_0$

. $B = A/(p)$ qui est intègre car p est inductible donc premier

. $L = Fr(B)$ (qui est un corps)

On projette (*) dans $B[X]$:

$$\overline{a_n} X^n = (\overline{b_q} X^q + \dots + \overline{b_0})(\overline{c_r} X^r + \dots + \overline{c_0}) = \overline{Q}\,\overline{R}$$

et l'égalité est alors également vraie dans $L[X]$.

Comme $L[X]$ est principal (donc factoriel) et X est inductible dans $L[X]$, par unicité de la décomposition en facteurs inductibles,

$X \mid \overline{a_n} X^n$ donc $X \mid \overline{Q}$ donc $\overline{b_0} = \overline{0}$

et $X \mid \overline{R}$ donc $\overline{c_0} = \overline{0}$

Par conséquent, $\begin{cases} p \mid b_0 \\ p \mid c_0 \end{cases}$ donc $p^2 \mid b_0 c_0 = a_0$ absurde

Donc, P est inductible dans $K[X]$.

Rq : On ne peut pas s'arrêter à la projection dans $B[X]$ pour conclure car $B = A/(p)$ n'a aucune raison d'être factoriel.

Par ex : $\mathbb{Z}[i\sqrt{5}] \simeq \mathbb{Z}[X]/(X^2+5)$ factoriel

pas factoriel : $9 = 3 \times 3 = (2+i\sqrt{5})(2-i\sqrt{5})$

(pas d'unicité de la décomposition en produit de facteurs inductibles)