Critère d'Eisenstein | Leçons : 122, 142

Thm : Soit A un anneau factoriel et $K = \mathrm{Frac}(A)$. $P(X) = a_n X^n + \dots + a_0 \in A[X]$ ~~avec $a_i \in A$~~
Soit $p \in A$ un élément irréductible. On suppose :
- $p \nmid a_n$ ▸ $p^2 \nmid a_0$ ▸ $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.

Alors P est irréductible dans $K[X]$.

Preuve :

$\boxed{\text{Etape 1}}$ On montre que le produit de deux polynômes primitifs de $A[X]$ est primitif.
Soit $\overset{P, Q}{A, B}$ primitifs et $C = \cancel{AB}\,PQ$ on suppose par l'absurde que C n'est pas primitif.
Donc il existe p premier qui divise tous les coefs c_k de C.
D'où $\overline{C} = 0$ dans $A/(p)[X]$ d'où $\cancel{\overline{A}\,\overline{B} = 0}$ $\overline{P}\,\overline{Q} = 0$ $\Rightarrow \overline{P}$ ou $\overline{Q} = 0$ par intégrité de $A/(p)$ d'où p divise tous les ~~éléments~~ coeffs de P ou Q, absurde car $c(A) = c(B) = 1$

$\boxed{\text{Etape 2}}$ On montre que si $\overset{\cancel{A,B}}{P, Q} \in A[X]$ alors $c(PQ) = c(P)c(Q)$

$$\text{On a } PQ = c(P)c(Q) \frac{P}{c(P)} \frac{Q}{c(Q)}$$, les polynômes $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$ sont primitifs

D'où leur produit aussi d'où $c(PQ) = c\left(c(P)c(Q) \frac{P}{c(P)} \frac{Q}{c(Q)}\right)$

$$= c(P)c(Q) \underbrace{c\left(\frac{P}{c(P)} \frac{Q}{c(Q)}\right)}_{=1} = c(P)c(Q)$$

$\boxed{\text{Etape 3}}$ On suppose P non irréductible sur $K[X]$.
On écrit $P = c(P)P'$ avec P' primitif et $P' = Q'R' \in K[X]$
On note q (resp r) le prod des dénominateurs des coeffs de Q' (resp de R')
D'où $Q = qQ'$ et $R = rR' \in A[X]$

D'où $qrP' = QR \Rightarrow qr = c(Q)c(R)$

$$\Rightarrow P = c(P) \frac{Q}{c(Q)} \cdot \frac{R}{c(R)} = \underbrace{\left(\frac{c(P)}{c(Q)} Q\right)}_{\in A[X]} \cdot \underbrace{\left(\frac{R}{c(R)}\right)}_{\in A[X]}.$$

On écrit donc $P = Q_1 R$ avec $Q, R \in A[X]$

On a $\begin{cases} Q = b_q X^q + \dots + b_0 \\ R = c_r X^r + \dots + c_0 \end{cases}$ où $1 \leq r, q \leq n-1$

A est factoriel et p irréductible $\Rightarrow (p)$ premier $\Rightarrow A/(p)$ intègre.
On projète l'égalité $P = QR$ dans $A/(p)[X]$ on a

$\overline{a_n} X^n = \overline{Q}\,\overline{R}$ cette égalité est tjrs vraie dans $\underbrace{\mathrm{Frac}(A/(p))}_{L}[X]$

L est un corps donc $L[X]$ est principal et en considérant le morphisme
$\varphi : \begin{cases} L[X] \to L \\ P \mapsto P(0) \end{cases}$ on a que $L[X]/(X) \simeq L$ d'où (X) est maximal

et donc X est irréductible et donc par unicité de la décomposition en polynôme irréductibles on a que $X | \overline{Q}$ et $X | \overline{R}$ d'où $\overline{b_0} = \overline{c_0} = 0$
D'où $p | b_0$ et $p | c_0 \Rightarrow p^2 | b_0 c_0 = c_0$ absurde, d'où l'irréductibilité de P.

$\square$

__Appli__ : $\phi_p = X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Z}[X]$

__Preuve__ : On a $\phi_p(X+1) = \cancel{(X+1)^p} \sum_{k=0}^{p-1} (X+1)^k = \frac{(X+1)^p - 1}{X}$

$$= \frac{1}{X}\left(\sum_{k=0}^{p} \binom{p}{k} X^k - 1\right)$$

$$= \frac{1}{X}\left(X^p + pX^{p-1} + \dots + pX\right) = \underset{\widehat{a}_{p-1}}{X^{p-1}} + \underset{\widehat{a}_{p-2}}{pX^{p-2}} + \dots + \underset{\widehat{a}_0}{p}$$

Par critère d'Eisenstein on a
- $p^2 \nmid a_0 = p$ et $p \nmid 1$
- $\forall k \in \{1, \dots, p-1\}$, $p | k! \binom{p}{k} \Rightarrow p | \binom{p}{k}$ car $p \wedge k! = 1$

D'où $p | a_i$ $\forall i \in \{0, \dots, p-2\}$
D'où ϕ_p est irr sur $\mathbb{Q}[X]$ et $c(\phi_p) = 1$ donc irr sur $\mathbb{Z}[X]$

$\square$.

FGN algèbre 1 + Perrin