CRITÈRE D'EISENSTEIN

[FGN07a, §5.16, p188–190]

ÉNONCÉ

PROPOSITION. [CRITÈRE D'EISENSTEIN]
Soit A un anneau factoriel. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. Supposons qu'il existe $p \in A$ premier tel que :

- $p \nmid a_n$,
- $p \mid a_i$ *pour tout* $i < n$,
- $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

DÉVELOPPEMENT

Soit A un anneau factoriel. Pour $P \in A[X]$, on note $c(P)$ un PGCD de ses coefficients.

Vérifions d'abord que si $P, Q \in A[X]$, alors $c(PQ) = c(P) \cdot c(Q)$.

- Traitons le cas $c(P) = c(Q) = 1$. Supposons par l'absurde $c(PQ) \neq 1$.
  On peut considérer p irréductible divisant $c(PQ)$. Alors p divise tous les coefficients de PQ, donc $0 = \overline{PQ} = \overline{P} \cdot \overline{Q}$ dans $A/(p)[X]$.
  Or p est irréductible donc est premier (puisque l'anneau A est factoriel), donc (p) est premier. En particulier $A/(p)$ puis $A/(p)[X]$ sont intègres. Ainsi $\overline{P} = 0$ ou $\overline{Q} = 0$, ou encore $p \mid c(P)$ ou $p \mid c(Q)$, ce qui est absurde.
- Dans le cas général, on remarque que $c(\alpha R) = \alpha \cdot c(R)$ pour tout $\alpha \in A$ et $R \in A[X]$.
  Écrivons $P = c(P) \cdot P'$, $Q = c(Q) \cdot Q'$ avec $c(P') = c(Q') = 1$. Alors :

$$c(PQ) = c(P) \cdot c(Q) \cdot c(P'Q') = c(P) \cdot c(Q)\,.$$

Revenons à P comme dans l'énoncé. Supposons-le non irréductible sur $\mathrm{Frac}(A)[X]$.

Écrivons $P = c(P)P'$ avec P' primitif puis $P' = Q'R'$ avec $Q', R' \in \mathrm{Frac}(A)[X]$ de degrés strictement inférieurs à $\deg(P)$. Notons q (respectivement r) le produit des dénominateurs des coefficients de Q' (respectivement R'). Alors $Q = qQ'$ et $R = rR'$ sont à coefficients dans A et $qrP' = QR$. En passant aux PGCD, on a $qr = c(Q) \cdot c(R)$, donc :

$$P = c(P) \cdot \frac{1}{c(Q)} \cdot Q \cdot \frac{1}{c(R)} \cdot R = \left(\frac{c(P)}{c(Q)} Q\right)\left(\frac{1}{c(R)} R\right),$$

et P s'écrit comme produit de deux polynômes de $A[X]$ de degrés inférieurs à P.

Écrivons $P = QR$ dans $A[X]$, avec Q et R de degrés respectifs ℓ et m strictement inférieurs à $\deg(P)$. Dans $A/(p)[X]$, on a alors

$$\overline{a_n} X^n = \overline{QR}\,.$$

Si $Q = \sum_{j=0}^{\ell} q_j X^j$ et $R = \sum_{k=0}^{m} r_k X^k$, on a $\overline{q_\ell} \neq 0$ et $\overline{r_m} \neq 0$ puisque $\overline{a_n} \neq 0$.
On peut alors considérer

$$j_0 = \min\Big(\big\{0 \leq j \leq \ell : \overline{q_j} \neq 0\big\}\Big) \quad \text{et} \quad k_0 = \min\Big(\big\{0 \leq k \leq m : \overline{r_k} \neq 0\big\}\Big)\,.$$

Si $j_0 + k_0 < n$, le monôme $X^{i_0+j_0}$ a pour coefficient $\overline{q_{j_0} r_{k_0}} \neq 0$ par intégrité, ce qui est absurde.

Ainsi $j_0 + k_0 = n$ et donc nécessairement $j_0 = \ell$ et $k_0 = m$. Autrement dit Q et R sont des monômes dans $A/(p)[X]$.

En particulier, $\overline{q_0} = \overline{r_0} = 0$, c'est-à-dire $p \mid q_0$ et $p \mid r_0$, et donc $p^2 \mid q_0 r_0 = a_0$, ce qui contredit l'hypothèse sur P.

Ainsi P est irréductible.

COMMENTAIRES

Certaines leçons nécessitent de considérer spécifiquement l'anneau $A = \mathbb{Z}$. La proposition s'écrit alors comme suit, et il faut adapter (et travailler !) les notations du développement.

PROPOSITION. [CRITÈRE D'EISENSTEIN]
Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. Supposons qu'il existe p entier premier tel que :

- $p \nmid a_n$,
- $p \mid a_i$ *pour tout* $i < n$,
- $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Q}[X]$.