

Soit A un anneau factoriel.

Lemme (de GAUSS) : Pour $P \in A[X]$, on note $c(P)$ un PGCD des coefficients de P . Pour tout $(P, Q) \in A[X]^2$, $c(PQ) = c(P)c(Q)$.

Thm (critère d'EISENSTEIN) : Supposons A intègre. Soit $P = a_0 + a_1X + \dots + a_nX^n \in A[X]$, $a_n \neq 0$. S'il existe $p \in A$ premier tel que $p \nmid a_n$, $p \mid a_0, \dots, p \mid a_{n-1}$ et $p^2 \nmid a_0$, alors P est irréductible dans $\text{Frac}(A)[X]$.

Preuve du Lemme : Supposons que $c(P) = c(Q) = 1$ et $c(PQ) \neq 1$. Il existe alors $\pi \in A$ irréductible qui divise tous les coefficients de PQ (car A est factoriel). Écrivons $P = \sum_{i=0}^r p_i X^i$ et $Q = \sum_{j=0}^s q_j X^j$. Comme $c(P) = c(Q) = 1$, il existe $i_0 \in \llbracket 1, r \rrbracket$ et $j_0 \in \llbracket 1, s \rrbracket$ tels que $\forall i < i_0, \forall j < j_0, \pi \nmid p_i, \pi \nmid q_j, \pi \nmid p_{i_0}$ et $\pi \nmid q_{j_0}$. Par hypothèse, $\pi \mid \sum_{i+j=i_0+j_0} p_i q_j = p_{i_0} q_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i < i_0 \text{ ou } j < j_0}} p_i q_j$ donc $\pi \mid p_{i_0} q_{j_0}$ par définition de i_0 et j_0 . Or π est aussi premier, donc $\pi \mid p_{i_0}$ ou $\pi \mid q_{j_0}$, ce qui est contradictoire. Donc $c(PQ) = 1 = c(P)c(Q)$.

Dans le cas général : il existe $\tilde{P} \in A[X]$ et $\tilde{Q} \in A[X]$ tels que $P = c(P)\tilde{P}$, $Q = c(Q)\tilde{Q}$, $c(\tilde{P}) = c(\tilde{Q}) = 1$. On a montré que $c(\tilde{P}\tilde{Q}) = c(\tilde{P})c(\tilde{Q}) = 1$, mais $PQ = c(P)c(Q)\tilde{P}\tilde{Q}$ donc $c(PQ) = c(P)c(Q)c(\tilde{P}\tilde{Q}) = c(P)c(Q)$ ■

Preuve du Thm : Posons $K = \text{Frac}(A)$. Par l'absurde, supposons qu'il existe $(Q, R) \in K[X]^2$ tel que $P = c(P)QR$ et $1 \leq \deg(Q) \leq \deg(R) < \deg(P)$. Il existe $(q, r) \in A^2$ tel que $qQ \in A[X]$ et $rR \in A[X]$. De là, $c(pqP) = c(c(P)qQrR)$, donc $pq c(P) = c(P) c(qQ) c(rR)$, donc $c(qQ) c(rR) = qr$. Finalement, $P = \frac{pq c(P)QR}{c(qQ) c(rR)} = \underbrace{\left[c(P) \frac{qQ}{c(qQ)} \right]}_{\in A[X]} \underbrace{\left[\frac{rR}{c(rR)} \right]}_{\in A[X]}$

(NB : $\frac{s}{c(s)} \in A[X]$ car $c(s) = \text{PGCD}(\text{coeffs de } s)$).

Il existe donc $(Q, R) \in A[X]^2$ tel que $P = QR$ et $1 \leq \deg(Q) \leq \deg(R) < \deg(P)$. Écrivons $Q = \sum_{k=0}^q b_k X^k$ et $R = \sum_{k=0}^r c_k X^k$, où $b_q \neq 0$ et $c_r \neq 0$. Comme p est premier, $A_{\langle p \rangle}$ est intègre. Dans $A_{\langle p \rangle}[X]$, $\bar{a}_n X^n = \bar{Q} \bar{R}$, en particulier $\bar{b}_q \bar{c}_r = \bar{a}_n \neq \bar{0}$, donc $\bar{b}_q \neq \bar{0}$ et $\bar{c}_r \neq \bar{0}$ par intégrité. On en déduit que $q = \deg(Q) = \deg(\bar{Q})$ et $r = \deg(R) = \deg(\bar{R})$. Toujours par intégrité, s'il existe $i < q$ tel que $\bar{b}_i \neq \bar{0}$, alors $\bar{Q} \bar{R} = \bar{b}_i \bar{c}_r X^{i+r} + \dots = \bar{a}_n X^n$, mais $i+r < q+r = n$, ce qui est absurde. Donc $\bar{Q} = \bar{b}_q X^q$ et de même $\bar{R} = \bar{c}_r X^r$. Comme $q = \deg(\bar{Q}) > 0$, on en déduit que $\bar{b}_0 = \bar{0}$, et de même $\bar{c}_0 = \bar{0}$, i.e. $p \mid b_0$ et $p \mid c_0$, donc $p^2 \mid b_0 c_0 = a_0$, ce qui contredit l'hypothèse.