# Critère d'Eisenstein

On suppose que $A$ est factoriel et on considère $\mathbb{K} = \mathrm{Frac}(A)$.

**Lemme 1.** *Le produit de deux polynômes primitifs est primitif.*

*Démonstration.*

Soient $P, Q \in A[X]$ deux polynômes primitifs. On suppose par l'absurde que $PQ$ n'est pas primitif.
Comme $A$ est factoriel, il existe donc $p \in A$ irréductible qui divise $c(PQ)$. Ainsi $(p)$ est un idéal premier, donc $A/(p)$ est intègre, et $A/(p)[X]$ aussi. Or $c(P) = c(Q) = 1$, donc $\overline{P}$ et $\overline{Q}$ ne sont pas nuls sur $A/(p)[X]$. Alors $\overline{PQ}$ n'est pas nul sur $A/(p)[X]$, et $p$ ne divise pas $PQ$. Contradiction. Donc $PQ$ est primitif. □

**Lemme 2.** *Pour $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

*Démonstration.*

On écrit $AB = c(A)c(B)\frac{A}{c(A)}\frac{B}{c(B)}$, où les polynômes $\frac{A}{c(A)}$ et $\frac{B}{c(B)}$ sont primitifs. Par le Lemme 1, leur produit est également primitif. On obtient alors, en passant au contenu, que $c(AB) = c(A)c(B)$. □

**Théorème 3.** *Soit $P \in A[X]$ non constant. Alors $P$ est irréductible dans $A[X]$ si, et seulement si, il est primitif et irréductible dans $\mathbb{K}[X]$.*

*Démonstration.*

($\Leftarrow$) Soit $P \in A[X]$ primitif et irréductible dans $\mathbb{K}[X]$.
Si $P(X) = Q(X)R(X)$ dans $A[X]$, c'est vrai aussi dans $\mathbb{K}[X]$.
Quitte à échanger $Q$ et $R$, comme $P$ est irréductible dans $\mathbb{K}[X]$, on suppose que $Q \in \mathbb{K}[X]^\times$, donc $\deg Q = 0$ et $Q \neq 0$. On a alors $Q = a \in A$. On en déduit que $P(X) = aR(X)$, donc $a \mid c(P)$.
Mais comme $c(P) = 1$, $a \in A^\times$, donc $P$ est irréductible.

($\Rightarrow$) Soit $P \in A[X]$ irréductible dans $A[X]$.
On a $c(P) = 1$, car sinon on peut écrire $P = pP'$ avec $p$ un irréductible de $A$ divisant $c(P)$.
On suppose par l'absurde que $P$ n'est pas irréductible. On a alors $P(X) = Q(X)R(X)$ avec $Q, R \in \mathbb{K}[X]$.
On écrit alors $Q(X) = \frac{a}{b}Q'(X)$ avec $Q' \in A[X]$ primitif et $a, b \in A$ premiers entre eux. Pour cela, on prend $b \in A$ un ppcm des dénominateurs des coefficients de $Q$, et $a \in A$ un pgcd des numérateurs des coefficients de $Q$, et on simplifie éventuellement la fraction $\frac{a}{b}$. On écrit de même $R(X) = \frac{c}{d}R'(X)$.
Ainsi, $bdP(X) = acQ(X)R(X)$, puis, en passant au contenu, $bd = ac$ modulo $A^\times$.
On a donc $P = \lambda Q'R'$, avec $\lambda \in A^\times$, mais comme $P$ est irréductible dans $A[X]$, $Q'$ ou $R'$ est dans $A[X]^\times = A^\times$, donc de degré 0, et $P$ est irréductible dans $\mathbb{K}[X]$.

□

**Théorème 4** (Eisenstein)**.** *Soit $P(X) = \sum_{k=1}^{n} a_k X^k \in A[X]$ non constant. On suppose qu'il existe $p \in A$ irréductible divisant tous les $a_k$ sauf $a_n$ et tel que $p^2$ ne divise pas $a_0$. Alors $P$ est irréductible dans $\mathbb{K}[X]$.*

*Démonstration.*

Supposons que $P$ est non irréductible dans $\mathbb{K}[X]$. Il existe alors $Q, R \in A[X]$ non constants tels que $P = QR$.
Posons alors $Q(X) = \sum_{k=0}^{q} b_k X^k$ et $R(X) = \sum_{k=0}^{r} c_k X^k$ avec $b_k, c_k \in A$ et $0 < q, r < n$.
Comme $A$ est factoriel et $p$ irréductible, l'idéal $(p)$ est premier, donc $B = A/(p)$ est intègre.
Projetons l'égalité $P = QR$ dans $B[X]$ :

$$\overline{P}(X) = \overline{a_n} X^n = \left( \sum_{k=0}^{q} \overline{b_k} X^k \right) \left( \sum_{k=0}^{r} \overline{c_k} X^k \right) = \overline{Q}(X)\overline{R}(X)$$

En effet, comme $\overline{a_n} \neq 0$, on a $\overline{b_q} \neq 0 \neq \overline{c_r}$. Cette égalité est encore vraie dans $\mathbb{L}[X]$, où $\mathbb{L} = \mathrm{Frac}(B)$.
Comme $\mathbb{L}[X]$ est principal et $X$ irréductible, l'unicité de la décomposition en facteurs irréductibles dans $\mathbb{L}[X]$ montre que $X$ divise $\overline{Q}$ et $\overline{R}$. Ainsi, $\overline{b_0} = \overline{c_0} = 0$ dans $B$, mais alors $p^2$ divise $b_0 c_0 = a_0$. Contradiction.

□

**Conclusion.** Le critère d'Eisenstein permet d'identifier facilement des polynômes irréductibles. ◁

## Références

[Per] Daniel Perrin. *Cours d'Algèbre.* Ellipses