# Critère d'Eisenstein.

Leçons: 122, 142, (141)

Réf: Perrin p51-76

Contenu de $P$ : pgcd des coefficients noté $c(P)$ défini modulo $A^*$.

**Lemme (Gauss):** si $A$ est factoriel, $P, Q \in A[X]$, alors $c(PQ) = c(P)c(Q)$ modulo $A^*$.

**Dém:**
- Montrons que si $P, Q$ sont primitifs alors $PQ$ est encore primitif. Supposons que $c(PQ) \neq 1$. Alors il existe $p \in A$ irréductible divisant $c(PQ)$ (car $A$ est factoriel). Comme $c(P) = c(Q) = 1$, il existe $i_0, j_0$ tq $\forall i < i_0$, $\forall j < j_0$, $p \mid a_i$, $p \mid b_j$ mais $p \nmid a_{i_0}$ et $p \nmid b_{j_0}$.
Par hyp. on a donc $p \mid c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j$
donc $p \nmid a_{i_0} b_{j_0}$ ce qui contredit le lemme d'Euclide.
- $PQ = c(P) \underbrace{\frac{P}{c(P)}}_{\text{primitifs}} c(Q) \frac{Q}{c(Q)}$ donc $c\left(\frac{PQ}{c(P)c(Q)}\right) = \frac{c(PQ)}{c(P)c(Q)} = 1$.

□

**Prop:** Les irréductibles de $A[X]$ sont :
i) les constantes $p \in A$ irréductibles dans $A$
ii) les polynômes $P \in A[X]$ de degré $\geq 1$, primitifs et irréductibles dans $K[X]$ avec $K = \mathrm{Frac}(A)$.

**Thm (Eisenstein):** $A$ factoriel, $K = \mathrm{Frac}(A)$, $P = \sum_{i=0}^{n} a_i X^i \in A[X]$, $p \in A$ irréductible.
On suppose : i) $p \nmid a_n$
ii) $\forall 0 \leq i \leq n-1$, $p \mid a_i$ et $p^2 \nmid a_0$.
Alors $P$ est irréductible dans $K[X]$ (donc dans $A[X]$ lorsque $c(P) = 1$) via la prop précédente.

**Dém:** Supposons que $P$ est réductible dans $K[X]$ : alors il l'est dans $A[X]$ donc on l'écrit $P = QR$ avec $Q, R \in A[X]$ avec $1 \leq \deg P, \deg Q < \deg P$.
$Q = b_q X^q + \dots + b_0$, $R = c_r X^r + \dots + c_0$, avec $q, r < n$, $b_i, c_j \in A$.

Comme $A$ est factoriel et $p$ est irréductible, $(p)$ est premier et $B = A/(p)$ est intègre. Posons $L = \mathrm{Frac}(B)$. On projète $P = QR$ dans $B[X]$ :

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

En outre, l'égalité reste vraie dans $L[X]$, qui lui est principal (donc factoriel) et comme $X$ est irréductible dans $L[X]$, l'unicité de la décomposition en facteurs irréductibles montre que $X$ divise $\overline{Q}$ et $\overline{R}$ donc que $\overline{b_0} = \overline{c_0} = 0$ dans $B$, mais alors $p^2 \mid a_0 = b_0 c_0$ ce qui contredit l'hypothèse.
Ainsi, $P$ est irréductible dans $K[X]$. □

Rmq : projeter dans $B[X]$ ne suffit pas car $B$ n'a aucune raison d'être factoriel.

Ex : $\underbrace{\mathbb{Z}[i\sqrt{5}]}_{\text{non factoriel}} \simeq \underbrace{\mathbb{Z}[X]}_{\text{factoriel}}/(X^2+5)$

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

Dém (prop) :

- Si $p \in A$ est irréductible avec $p = Q(X)R(X)$, on a $\deg Q = \deg R = 0$ donc $Q, R \in A$ et l'un d'eux est dans $A^*$ donc est inversible dans $A[X]$ donc $p$ est irréductible dans $A[X]$.
- Si $P$ est primitif et irréductible dans $K[X]$, on écrit $P(X) = Q(X)R(X)$ dans $A[X]$ et donc dans $K[X]$. Comme $P$ est irréductible, on a par exemple $Q \in K[X]^*$ donc $\deg Q = 0$ et $Q \neq 0$.
  Donc $Q = a \in A$ si bien que $P = aR$ donc $a \mid c(P) = 1$ donc $a \in A^*$ donc $P$ est irréductible dans $A[X]$.

- Montrons que ce sont les seuls irréductibles. Soit $P$ irréductible dans $A[X]$. Si $\deg P = 0$, $P = p \in A$ est nécessairement irréductible dans $A$.
  Si $\deg P > 0$, on a nécessairement $c(P) = 1$. Sinon on peut écrire $P = aQ$ avec $a \notin A^* = A[X]^*$ et $\deg Q = \deg P > 0$ donc $Q \notin A^* = A[X]^*$.

- Montrons que $P$ est irréductible dans $K[X]$.

Si $P = QR$ dans $K[X]$.
Il existe $a, b \in A$ premiers entre eux tq $Q = \frac{a}{b}\tilde{Q}$ avec $\begin{cases} \tilde{Q} \in A[X] \\ c(\tilde{Q}) = 1 \end{cases}$

$c, d \in A$ _____ $R = \frac{c}{d}\tilde{R}$ avec $\begin{cases} \tilde{R} \in A[X] \\ c(\tilde{R}) = 1 \end{cases}$

(Si $Q(X) = \sum_{i=1}^{n} \frac{a_i}{b_i} X^i$, $a = \text{pgcd}(a_i)$, $b = \text{ppcm}(b_i)$ puis on simplifie éventuellement la fraction $\frac{a}{b}$)

On a alors $bdP = ac\tilde{Q}\tilde{R}$ donc d'après le Lemme (de Gauss),
$c(bdP) = bd = c(ac\tilde{Q}\tilde{R}) = ac\, c(\tilde{Q})c(\tilde{R}) = ac$ modulo $A^*$
Donc $\lambda = \frac{ac}{bd} \in A^*$ donc $P = \lambda\tilde{Q}\tilde{R}$ dans $A[X]$.

Comme $P$ est irréductible dans $A[X]$ donc $\tilde{Q}$ ou $\tilde{R}$ est dans $A[X]^* = A^*$

donc $\deg\tilde{Q} = \deg Q = 0$ ou $\deg\tilde{R} = \deg R = 0$
donc $Q \in K^* = K[X]^*$ (ou $R$...)
donc $P$ est irréductible dans $K[X]$. □

Appli :
- souvent $A = \mathbb{Z}$, $K = \mathbb{Q}$.
- $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ pour tout $n \geq 1$ : contrairement au cas réel ou complexe, il existe des polynômes irréductibles de degré aussi grand qu'on veut dans $\mathbb{Q}[X]$.
- $\Phi_p$ est irréductible dans $\mathbb{Q}[X]$ : $\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$.

Or pour $k \neq 1$, $k\binom{p}{k} = p\binom{p-1}{k-1}$ montre que (pour $k < p$), $p \mid \binom{p}{k}$ par le Lemme de Gauss. Et $p^2 \nmid \binom{p}{1} = p$ donc on peut appliquer Eisenstein. Donc $\Phi_p(X+1)$, et donc $\Phi_p$, est irréductible.

Si $P \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, il est irréductible dans $\mathbb{Q}[X]$.

Si $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ et $\deg Q, \deg R \geqslant 1$.
En chassant les dénominateurs, il existe $q, r \in \mathbb{Z}$ tq $qQ, rR \in \mathbb{Z}[X]$.
On obtient alors $qrP = qQ\, rR = c(qQ)\, \underbrace{\widetilde{qQ}}_{\text{primitifs}}\, c(rR)\, \underbrace{\widetilde{rR}}_{\text{primitifs}}$.

D'après le lemme (de Gauss),

$$qr\, c(P) = c(qQ)\, c(rR) \text{ donc } P = c(P)\, \underbrace{\widetilde{qQ}}_{\deg \geqslant 1}\, \underbrace{\widetilde{rR}}_{\deg \geqslant 1} \text{ et dans } \mathbb{Z}[X]$$

ce qui contredit le fait que $P$ soit irréductible dans $\mathbb{Z}[X]$. □