1 Critère d'Eisenstein

Abstract

Le critère d'Eisenstein est un critère d'irréductibilité d'un polynôme. Dans sa forme la plus connue, il s'énonce ainsi : soit $P = \sum_{i=0}^{d} a_i X^i$ un polynôme à coefficients dans $\mathbb{Z}$. S'il existe un nombre premier p tel que p divise tous les coefficients sauf le dernier et que p^2 ne divise pas le premier coefficient, alors P est irréductible dans $\mathbb{Q}[X]$.

Nous en donnerons une généralisation dans le cas des polynômes à coefficients dans un anneau intègre.

Définition 1. *Soit $\mathcal{A}$ un anneau commutatif. Un idéal I est dit premier si pour tous $a, b \in \mathcal{A}$, si $ab \in I$, alors $a \in I$ ou $b \in I$.*

Remarque 1. *De manière équivalente, un idéal I est dit premier si $\mathcal{A}/I$ définit par passage au quotient un anneau intègre.*

Théorème 1 (Critère d'Eisenstein)**.** *Soit $\mathcal{A}$ un anneau intègre. Soit $P = \sum_{i=0}^{d} a_i x^i \in \mathcal{A}[x]$. S'il existe un idéal premier I de $\mathcal{A}$ tel que*

- *$\forall i \in \{0, ..., d-1\}, a_i \in I$,*
- *$a_d \notin I$,*
- *$a_0 \notin I^2$ (c'est-à-dire a_0 n'est pas le carré d'un élément de I),*

Alors P est irréductible dans $\mathcal{A}[x]$.

Proof. Supposons que $P = RQ$ avec $\deg(R) = m$ et $\deg(Q) = d - m$ avec $\deg(R) \geq 1$. Par réduction modulo I (i.e. considérer $\mathcal{A}/I[x]$), on a

$$P = RQ = a_d x^d \bmod I. \tag{1}$$

Or $\mathcal{A}/I$ est intègre donc $\mathcal{A}/I[x]$ est intègre. On en déduit que les réductions de R et Q sont de la forme $R = bx^m \bmod I$ et $Q = cx^{d-m} \bmod I$. En particulier, on en déduit que r_0 et g_0 sont dans I. Puisque $a_0 = r_0 g_0$, on en déduit que $a_0 \in I^2$. Cela contredit l'hypothèse du théorème, on en déduit que P est irréductible. □

Le théorème d'Eisenstein pour les polynômes à coefficients dans $\mathbb{Z}$ est un peu plus fort que le théorème général puisqu'on obtient une irréductibilité dans $\mathbb{Q}[X]$ et non dans $\mathbb{Z}[X]$. C'est l'objet de la proposition suivante, qui montre que les deux théorèmes sont équivalents.

Proposition 1. *Un polynôme $P \in \mathbb{Z}[X]$ est irréductible dans $Q[X]$ si et seulement si il est irréductible dans $\mathbb{Z}[X]$.*

Proof. Bien sûr, si P est irréductible dans $\mathbb{Q}[X]$, il est aussi dans $\mathbb{Z}[X]$. Supposons désormais qu'il le soit dans $\mathbb{Z}[X]$. Supposons qu'il existe $R, Q \in \mathbb{Q}[X]$ tels que $P = RQ$.

Il existe $q, r \in \mathbb{Z}$ tel que $qQ \in \mathbb{Z}[X]$ et $rR \in \mathbb{Z}[X]$. On peut ensuite écrire

$$qrP = qRrQ = c(qR)R'c(rQ)Q' \tag{2}$$

où R', Q' sont des polynômes à coefficients entiers et $c(R), c(Q)$ sont les pgcd des coefficients de R et Q. On en déduit que

$$qrc(P) = c(qR)c(rQ) \tag{3}$$

d'où $qrP = qrc(P)R'Q'$ et finalement que $P = c(P)R'Q'$. En conclusion, P est irréductible dans $\mathbb{Z}[X]$ puisque R', Q' sont de degrés supérieurs à 1, et $c(P)$ n'est qu'une constante entière. □

Corollaire 1 (Critère d'Eisenstein)**.** *Soit $P = \sum_{i=0}^{d} a_i X^i$ un polynôme à coefficients dans $\mathbb{Z}$. S'il existe un nombre premier p tel que p divise tous les coefficients sauf le dernier et que p^2 ne divise pas le premier coefficient, alors P est irréductible dans $\mathbb{Q}[X]$.*

Proof. On applique le théorème d'Eisenstein avec $\mathcal{A} = \mathbb{Z}$ et $I = (p)$. Ainsi, P est irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$ par la proposition précédente. □

Le critère d'Eisenstein est un critère d'irréductibilité puissant, en particulier lorsque l'on considère les fermés de Zariski. L'idée est de considérer $\mathcal{A}[x, y]$ comme $\mathcal{A}[x][y]$ et d'appliquer le critère d'Eisenstein sur $\mathcal{A}[x]$.

Exemple 1. *Soit $f = y^2 + yx^2 + x$. On peut considérer $I = (x)$. $f_0 = x \in I$ et $f_0 = x \notin I^2$, $f_1 = x^2 \in I$ et $f_2 = 1 \notin I$. On en déduit que f est irréductible dans $\mathbb{C}[x][y]$.*

De manière générale, on a le corollaire suivant :

Corollaire 2. *Soit $f \in \mathcal{A}[x, y]$ sous la forme $f = \sum_{i=0}^{d} f_i(x) y^i$. Si les f_i sont premiers entre eux et qu'il existe un polynôme irréductible $p(x)$ tel que $p(x)$ divise tous les f_i sauf le dernier et que $p^2(x)$ ne divise pas f_0, alors f est irréductible dans $\mathcal{A}[x, y]$.*

Le critère d'Eisenstein s'applique plus souvent sur des polynômes à coefficients entiers. On peut par exemple établir l'irréductibilité du p-ième polynôme cyclotomique.

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + 1. \tag{4}$$

Corollaire 3. *Le p-ième polynôme cyclotomique est irréductible dans $\mathbb{Q}[X]$.*

Proof. On calcule d'abord $\Phi_p(X + 1)$

$$\Phi_p(X + 1) = \frac{(X + 1)^P - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}. \tag{5}$$

D'après le critère d'Eisenstein avec p, $\Phi_p(X+1)$ est irréductible dans $\mathbb{Q}[X]$. (p divise $\binom{p}{i}$ pour $i \in \{1, ..., p-1\}$, p^2 ne divise pas $\binom{p}{1}$ et p ne divise pas $\binom{p}{p}$). Si Φ_p était réductible, alors il existerait $R, Q \in \mathbb{Q}[X]$ tels que $\Phi_p = RQ$. On aurait alors

$$\Phi_p(X+1) = R(X+1)Q(X+1) = R'(X)Q'(X). \tag{6}$$

Ce qui contredirait l'irréductibilité de $\Phi_p(X+1)$. □

On conclut par un dernier corollaire intéressant.

Corollaire 4. $\mathbb{Q}[X]$ *admet des polynômes irréductibles de degré arbitrairement grand.*

Proof. On pose $P_n = X^n - 2$. On a directement par le critère d'Eisenstein que P_n est irréductible dans $\mathbb{Q}[X]$. □