

Critère d'Eisenstein

Leçons : 122, 125, 141

Référence : X. Gourdon, *Algèbre*, 3^e édition.

On rappelle que pour $P \in \mathbb{Z}[X] \setminus \{0\}$, le *contenu* de P , noté $c(P)$, est le pgcd des coefficients de P .

Lemme 1 (Lemme de Gauss). *Soit $P, Q \in \mathbb{Z}[X]$. Alors,*

$$c(P) c(Q) = c(PQ).$$

Démonstration. On a $P_1 = \frac{1}{c(P)}P$ et $Q_1 = \frac{1}{c(Q)}Q$ dans $\mathbb{Z}[X]$, et $c(P_1) = c(Q_1) = 1$.

Si $c(P_1 Q_1) > 1$ alors il existe p premier tel que $p \mid c(P_1 Q_1)$. Donc p divise tous les coefficients de $P_1 Q_1$. Donc, $p \mid c(P_1)$ ou $p \mid c(Q_1)$, ce qui est absurde car $c(P_1) = c(Q_1) = 1$ et p est premier. Donc,

$$c(P_1 Q_1) = 1.$$

Donc,

$$\begin{aligned} c(PQ) &= c(c(P)P_1 c(Q)Q_1) \\ &= c(P) c(Q). \end{aligned}$$

CQFD

Lemme 2. *Si φ est irréductible dans $\mathbb{Z}[X]$, alors φ est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Soit $\varphi \in \mathbb{Z}[X]$. Notons $\varphi = PQ$. Montrons que P ou Q est constant.

Soit $\alpha, \beta \in \mathbb{N}^*$ tels que $P_1 = \alpha P$ et $Q_1 = \beta Q$ soient dans $\mathbb{Z}[X]$. Donc,

$$P_1 Q_1 = \alpha \beta P Q = \alpha \beta \varphi.$$

Par le lemme de Gauss,

$$\alpha \beta c(\varphi) = c(P_1) c(Q_1).$$

Posons alors $P_2 = \frac{1}{c(P_1)}P_1$ et $Q_2 = \frac{1}{c(Q_1)}Q_1$. $P_2, Q_2 \in \mathbb{Z}[X]$ et,

$$\begin{aligned} \alpha \beta \varphi &= P_1 Q_1 = c(P_1) c(Q_1) P_2 Q_2 \\ &= \alpha \beta c(\varphi) P_2 Q_2. \end{aligned}$$

φ est irréductible sur $\mathbb{Z}$ donc $c(\varphi)P_2$ est constant ou Q_2 est constant, non nul. Mais alors P_1 ou Q_1 l'est, et donc P ou Q l'est.

Donc,

$\varphi \text{ est irréductible dans } \mathbb{Q}[X].$

CQFD

Théorème 3 (Critère d'Eisenstein). *Soit $P = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathbb{Z}$ un élément premier. On suppose que :*

① $p \nmid a_n$.

② $p \mid a_i, \forall i \in \llbracket 0, n-1 \rrbracket$.

③ $p^2 \nmid a_0$.

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

Démonstration. Par contraposée, supposons P réductible dans $\mathbb{Q}[X]$. D'après le lemme, P est donc réductible dans $\mathbb{Z}[X]$.

Soit donc $Q, R \in \mathbb{Z}[X]$ tels que $P = QR$ avec $\deg(Q), \deg(R) \geq 1$.

En passant dans $\mathbb{Z}/p\mathbb{Z}$, on a donc,

$$\overline{P} = \overline{a_n} X^n.$$

Notons $Q = \sum_{i=0}^a q_i X^i$ et $R = \sum_{i=0}^b r_i X^i$. On a alors,

$$\overline{P} = \overline{Q} \overline{R} = \overline{a_n} X^n,$$

donc,

$$\overline{Q} = \overline{q_a} X^a \quad \text{et} \quad \overline{R} = \overline{r_b} X^b.$$

Donc, $\overline{q_0} = \overline{r_0} = 0$. Donc, $p \mid q_0, p \mid r_0$, donc $p^2 \mid q_0 r_0 = a_0$, ce qui contredit l'hypothèse ③.

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