Développement : Lemme de Gauss et critère d'Eisenstein

Référence : Gourdon, Algèbre
Leçon : 120, 121, 122, 125, 141 et 142.

Lemme :
Soient $P, Q \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que p divise tous les coefficients du produit PQ. Alors, p divise tous les coefficients de P ou tous les coefficients de Q.

Démonstration. Si $a \in \mathbb{Z}$, on note $\bar{a}$ sa classe dans $\mathbb{Z}/p\mathbb{Z}$. Si $P = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, on note $\overline{P} = \bar{a}_n X^n + \cdots + \bar{a}_1 X + \bar{a}_0 \in \mathbb{Z}/p\mathbb{Z}[X]$. Si p divise tous les coefficients de PQ, on a, avec ces notations : $\overline{PQ} = \overline{P} \cdot \overline{Q} = \overline{0}$. Comme $\mathbb{Z}/p\mathbb{Z}$ est intègre, $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre. Donc $\overline{P} = \overline{0}$ ou $\overline{Q} = \overline{0}$, d'où le résultat. □

Lemme : (Lemme de Gauss)
Si $P \in \mathbb{Z}[X]$, on note $c(P)$ le pgcd des coefficients de P (et $c(P) = 1$ si $P = 0$). Alors $c(PQ) = c(P)c(Q)$.

Démonstration. Soient $P, Q \in \mathbb{Z}[X]$. Il est clair que $P_1 = \frac{1}{c(P)}P$ et $Q_1 = \frac{1}{c(Q)}Q$ sont dans $\mathbb{Z}[X]$, et on a $c(P_1) = c(Q_1) = 1$. Si $c(P_1Q_1) > 1$, alors il existe un nombre premier p divisant $c(P_1Q_1)$. D'après le lemme précédent, on a donc $p \mid c(P_1)$ ou $p \mid c(Q_1)$, ce qui est absurde. Donc $c(P_1Q_1) = 1$, ce qui entraîne $c(PQ) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q)$. □

Théorème : (Critère d'Eisenstein)
Soit $n \in \mathbb{N}^*$ et $P = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que

$$(i) \quad \forall k,\ 0 \leq k \leq n-1,\ p \mid a_k \qquad (ii) \quad p \nmid a_n \qquad (iii) \quad p^2 \nmid a_0.$$

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

Démonstration. Supposons P réductible dans $\mathbb{Q}[X]$.

Il existe $P, Q \in \mathbb{Q}[X]$ tels que $\Phi = PQ$ avec $a = \deg(Q) \geq 1$ et $b = \deg(R) \geq 1$.

Soient $\alpha, \beta \in \mathbb{N}^*$ tels que $P_1 = \alpha P$ et $Q_1 = \beta Q \in \mathbb{Z}[X]$. On a $\alpha\beta\Phi = P_1Q_1$ donc d'après le lemme de Gauss

$$\alpha\beta \cdot c(\Phi) = c(P_1)c(Q_1).$$

Posons $P_2 = \frac{1}{c(P_1)}P_1$ et $Q_2 = \frac{1}{c(Q_1)}Q_1$. Ces polynômes sont à coefficients entiers. Par ailleurs,

$$\alpha\beta\Phi = c(P_1)c(Q_1)P_2Q_2 = \alpha\beta \cdot c(\Phi)P_2Q_2.$$

Si $P_3 = c(\Phi)P_2$, on a donc $\Phi = P_3Q_2$ avec $P_3, Q_2 \in \mathbb{Z}[X]$. On remarque que $\deg(P_3) = \deg(P) = a \geq 1$ et $\deg(Q_2) = \deg(Q) = b \geq 1$.

Dans $\mathbb{Z}/p\mathbb{Z}$, on a, d'après les hypothèses, $\overline{P} = \bar{a}_n X^n$. Écrivons

$$\overline{Q} = \sum_{i=0}^{a} \bar{q}_i X^i \quad \text{et} \quad \overline{R} = \sum_{i=0}^{b} \bar{r}_i X^i.$$

Dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a $\overline{P} = \overline{QR}$ donc $\bar{a}_n X^n = \overline{QR}$, donc $\overline{Q} = \bar{q}_a X^a$ et $\overline{R} = \bar{r}_b X^b$. Ceci entraîne $\bar{q}_0 = \bar{r}_0 = \bar{0}$, donc $p \mid q_0$ et $p \mid r_0$, donc $p^2 \mid q_0 r_0 = a_0$, ce qui est contraire aux hypothèses. Finalement, P est irréductible dans $\mathbb{Q}[X]$. □

Application
Soit p un nombre premier et $\Phi(X) = X^{p-1} + \cdots + X + 1$. On a Φ est irréductible dans $\mathbb{Q}[X]$.

Démonstration. L'astuce est d'utiliser le critère d'Eisenstein en considérant $\Phi(X+1)$. L'identité $(X-1)\Phi(X) = X^p - 1$ entraîne $X\Phi(X+1) = (X+1)^p - 1$, d'où on tire

$$\Phi(X+1) = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}.$$

Il est maintenant facile de vérifier que $\Phi(X+1)$ satisfait les hypothèses du critère d'Eisenstein avec le nombre premier p (rappelons que si p est premier et si $1 \leq k \leq p-1$, alors $p \mid \binom{p}{k}$), donc $\Phi(X+1)$ est irréductible dans $\mathbb{Q}[X]$. Donc $\Phi(X)$ est irréductible dans $\mathbb{Q}[X]$. □