X. G Algèbre

p62.

Développement : Critère d'Eisenstein

122

125

141

142

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

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

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

Preuve :

① Si $a \in \mathbb{Z}$ on note $\bar{a}$ sa classe dans $\mathbb{Z}/p\mathbb{Z}$. Si $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ on note $\bar{P} = \bar{a}_n X^n + \dots + \bar{a}_1 X + \bar{a}_0 \in \mathbb{Z}/p\mathbb{Z}[X]$. Si $p \mid c(PQ)$, on a avec ces notations $\bar{P}\bar{Q} = \bar{P}\bar{Q} = \bar{0}$. Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est intègre donc $\mathbb{Z}/p\mathbb{Z}[X]$ aussi. Donc $\bar{P} = 0$ ou $\bar{Q} = 0$ et $p \mid c(P)$ ou $c(Q)$.

② Lemme de Gauss, si $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)\,c(Q)$.

Soient $P, Q \in \mathbb{Z}[X]$. Il est clair que $P_1 = \frac{P}{c(P)}$ et $Q_1 = \frac{Q}{c(Q)} \in \mathbb{Z}[X]$ et on a $c(P_1) = c(Q_1) = 1$. Si $c(P_1 Q_1) > 1$, il existe p premier divisant $c(P_1 Q_1)$ (théorème d'Euclide) D'après ②, $p \mid c(P_1)$ ou $c(Q_1)$ ie $p \mid 1$, ABS.

Donc $c(P_1 Q_1) = 1$ et $c(PQ) = c(P)c(Q)\,c(P_1 Q_1) = c(P)\,c(Q)$.

③ Mq si $\Phi \in \mathbb{Z}[X]$ irr sur $\mathbb{Z}[X]$ alors Φ irr sur $\mathbb{Q}[X]$.

Soient P et $Q \in \mathbb{Q}[X]$ tq $\Phi = PQ$. Soient α et $\beta \in \mathbb{N}^*$ tq $P_1 = \alpha P$ et $Q_1 = \beta Q \in \mathbb{Z}[X]$ (α (resp β) le produit des dénominateurs de P (resp Q) convient). On pose $P_2 = \frac{P_1}{c(P_1)}$ et $Q_2 = \frac{Q_1}{c(Q_1)} \in \mathbb{Z}[X]$. Alors :

$$\alpha\beta\,\Phi = c(P_1)\,c(Q_1)\,P_2 Q_2 = \alpha\beta\,c(PQ)\,P_2 Q_2.$$

On pose $P_3 = c(\Phi)\,P_2 \in \mathbb{Z}[X]$ et $\Phi = P_3 Q_2$ avec P_3 et $Q_2 \in \mathbb{Z}[X]$. Comme Φ est irréductible dans $\mathbb{Z}[X]$, $d^\circ P_3 = d^\circ P = 0$ ou $d^\circ Q_2 = d^\circ Q = 0$ d'où le résultat.

④ On montre le critère d'Eisenstein.

Supposons P réductible dans $\mathbb{Q}[X]$, d'après ③, P est réductible dans $\mathbb{Z}[X]$ donc il existe $Q, R \in \mathbb{Z}[X]$ tels que $P = QR$, avec $a = d^\circ Q \geq 1$ et $b = d^\circ R \geq 1$.

Dans $\mathbb{Z}/p\mathbb{Z}$, on a, d'après les hypothèses $\bar{P}(X) = \bar{a}_m X^m = (\bar{b}_a X^a + \dots + \bar{b}_0)(\bar{c}_b X^b + \dots + \bar{c}_0)$

⚠ Comme X est irréductible, si $X \mid \bar{b}_a X^a + \dots + \bar{b}_0$ mais pas $\bar{R}$ alors $X^m \mid \bar{Q}$ pour des raisons de degrés et $\bar{R}$ est de $d^\circ = 0$, ABS donc $X \mid \bar{Q}$ et $X \mid \bar{R}$, ie $\bar{b}_0 = \bar{c}_0 = 0$ et $p^2 \mid c_0 b_0 = a_0$, C'est contraire aux hypothèses donc P est irréductible dans $\mathbb{Q}[X]$.

⑤ Application : Soit p 1er et $\Phi_p(X) = X^{p-1} + \dots + 1$. Mq Φ_p est irr ds $\mathbb{Q}[X]$.

On considère $\Phi_p(X+1)\,X = (X+1)^p - 1$.

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

et $\Phi_p(X+1)$ satisfait les hyp du critère d'Eisenstein avec le nb 1er p (rappelons que si $1 \le k \le p-1$, alors $p \mid \binom{p}{k}$) donc $\Phi_p(X+1)$ est irréductible dans $\mathbb{Q}[X]$ et donc $\Phi_p(X)$ est irréductible dans $\mathbb{Q}[X]$.

Remarque : $c(\Phi_p) = 1$ donc Φ_p est irr sur $\mathbb{Z}[X]$.