# Developpement : critère d'Eisenstein.

• Rombaldi p383
Victoire p 205

Soit $P = p_n X^n + \dots + p_1 X^1 + p_0 \in \mathbb{Z}[X]$ et $p$ premier

On suppose que i) $p \nmid p_n$

ii) $p \mid p_i$ : $\forall i \in [\![0, n-1]\!]$

iii) $p^2 \nmid p_0$

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

① Définition du contenu

② Produit de 2 polynômes primitifs dans $\mathbb{Z}[X] \setminus \{0\}$ est primitif.

③ $P, Q \in \mathbb{Z}[X] \setminus \{0\}$ $c(PQ) = c(P)\,c(Q)$

④ $P \in \mathbb{Z}[X]$, si $P$ est réductible dans $\mathbb{Q}[X]$, il s'écrit sous la forme

$P = QR$ avec $Q, R \in \mathbb{Z}[X]$

(⑤ $P, Q$ 2 polynômes unitaires de $\mathbb{Q}[X]$ tel que $PQ \in \mathbb{Z}[X]$ alors $P, Q \in \mathbb{Z}[X]$)

⑥ conclusion.

① Définition du contenu.

Notons $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X] \setminus \{0\}$

le contenu $\underline{c(P) = \text{pgcd}(a_0, \dots, a_n)}$

on dit que $P$ est primitif si son contenu est égal à 1

(Remarques : $p$ premier $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est 1 corps

On note $\bar{P}(X) = \sum_{k=0}^{n} \bar{a}_k X^k$ dans $\mathbb{Z}/p\mathbb{Z}[X]$

avec $\bar{a}_k$ classe de $a_k$ dans $\mathbb{Z}/p\mathbb{Z}$

Rombaldi p381 ① $p$ premier, $A_1, \dots A_k$ polynômes de $\mathbb{Z}[X]$

et $A = \sum_{j=1}^{k} A_j$, on a dans $\mathbb{F}_p$ :

$$\overline{A^p} = \sum_{j=1}^{h} \overline{A_j^p}$$

② $A \in \mathbb{Z}[X]$, $B = A^p$, dans $\mathbb{Z}/p\mathbb{Z}[X]$ $\overline{B}(X) = \overline{A}(X^p)$

preuve : ① par récurrence, $h = 2$

$p$ premier, $p \mid \binom{p}{j}$ $j \in [\![1, p-1]\!]$ car $p \mid p! = j!(p-j)! \binom{p}{j}$

et $p \wedge j!(p-j)!$, d'après Gauss $p \mid \binom{p}{j}$

dans $\mathbb{Z}/p\mathbb{Z}[X]$ $\overline{(A_1 + A_2)^p} = \sum_{j=0}^{p} \binom{p}{j} \overline{A_1}^j \overline{A_2}^{p-j} = \overline{A_1}^p + \overline{A_2}^p$

(récurrence immédiate)

③ $A(X) = \sum_{k=0}^{n} a_k X^k$ dans $\mathbb{Z}[X]$ et $B = A^p$

Avec le résultat précédent, dans $\mathbb{Z}/p\mathbb{Z}[X]$

$$\overline{B}(X) = \overline{\left(\sum_{k=0}^{n} a_k X^k\right)^p} = \sum_{k=0}^{n} \overline{a_k}^p X^{kp}$$

et $\overline{a_k}^p = \overline{a_k}^{\,p} = \overline{a_k}$ dans $\mathbb{Z}/p\mathbb{Z}$ par le th. de Fermat.

d'où $\overline{B}(X) = \sum_{k=0}^{n} \overline{a_k} X^{kp} = \overline{A}(X^p)$

④ Produit de deux polynômes primitifs est primitif.

Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$ primitifs

notons $R(X) = \sum_{k=0}^{m+n} c_k X^k$

Raisonnons par l'absurde, supposons que $R$ n'est pas primitif.

$c(P)$ admet un diviseur premier $p$ tq $p \mid c_k$ $\forall k \in [\![0, m+n]\!]$

$c(R)$

d'où dans $\mathbb{Z}/p\mathbb{Z}[X]$

$$\overline{R}(X) = \sum_{k=0}^{n+m} \overline{c_k} X^k = \overline{0}$$

donc $\overline{R} = \overline{Q}\,\overline{P} = \overline{0} \Rightarrow \overline{Q} = \overline{0}$ ou $\overline{P} = \overline{0}$

car $p$ premier $\mathbb{Z}/p\mathbb{Z}$ est 1 corps donc aussi intègre (à chercher pour $\mathbb{Z}/p\mathbb{Z}[X]$)

d'où $p$ divise tous les coeff de $P$

tous les coeff de $Q$

Absurde car $P, Q$ sont primitifs

Donc le produit de 2 polynômes primitifs est primitif.

(note chaque coeff $c_k = \sum_{j=0}^{k} a_j \cdot b_{k-j}$)

2ème note : $A$ anneau intègre $\Rightarrow$ $A[X]$ intègre

$(P, Q) \in (A[X] \setminus \{0\})^2$ deg $P = k$ deg $Q = \ell$

coeff dominant de $PQ$ : $a_k b_\ell$

de plus ces coeff dominant $\neq 0$ $a_k \neq 0$ $b_\ell \neq 0$

ce $A$ est intègre $a_k b_\ell \neq 0$ donc $PQ \neq 0$

$A[X]$ est intègre.

③ $\forall P, Q \in \mathbb{Z}[X] \setminus \{0\}$ $c(PQ) = c(P)\, c(Q)$

en effet $P \cdot Q = c(P)\, c(Q) \left(\frac{P}{c(P)}\right)\left(\frac{Q}{c(Q)}\right)$

avec $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$ primitifs et à coeff dans $\mathbb{Z}$

car

$PQ = c(P)\, c(Q)\, R$ avec $R$ primitif (cf q. puc)

et avec homogénéité du pgcd $(\text{pgcd}(da_0, \dots, da_n) = d\,\text{pgcd}(a_0, \dots, a_n))$

$$c(PQ) = c\Big(\underbrace{c(P)\, c(Q)}_{\lambda} \frac{P}{c(P)} \frac{Q}{c(Q)}\Big)$$

$$= c(P)\, c(Q)\, c\Big(\underbrace{\frac{P}{c(P)} \frac{Q}{c(Q)}}_{\text{primitif donc } c(\cdot) = 1}\Big)$$

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

④ $P \in \mathbb{Z}[X]$ . $P$ réductible dans $\mathbb{Q}[X] \Rightarrow$ réductible dans $\mathbb{Z}[X]$

$P = c(P) P_1$ avec $P_1$ primitif dans $\mathbb{Z}[X]$

Si $P$ est réductible dans $\mathbb{Q}[X]$ alors $P_1$ aussi :

donc $P_1 = Q_1 R_1$ avec $Q_1, R_1 \in \mathbb{Q}[X]$ non constants

Posons $q$ le produit des dénominateurs des coeffs de $Q_1$ $(\neq 0)$

$r$ le produit des dénominateurs des coeffs de $R_1$ $(\neq 0)$

On introduit $\begin{cases} Q_1 = \frac{1}{q} Q_2 \\ R_1 = \frac{1}{r} R_2 \end{cases}$ , $Q_2, R_2 \in \mathbb{Z}[X]$ par construction.

$Q_2 R_2 = qr\, Q_1 R_1 = qr\, P_1$

On passe au contenu.

$c(qr P_1) = qr\, c(P_1) = c(Q_2 R_2) = c(Q_2)\, c(R_2) = qc(Q_1)\, r c(R_1)$

$= qr\, \underbrace{c(Q_1)}_{\in \mathbb{Z}}\, \underbrace{c(R_1)}_{\in \mathbb{Z}}$

$qr = qr\, c(Q_1) c(R_1)$ donc $c(Q_1) = c(R_1) = 1$ *

$\Rightarrow P = c(P) P_1 = c(P)\, Q_1 R_1$

$P = \frac{c(P)}{qr} Q_2 R_2$

$P = c(P) \frac{Q_2}{q} \times \frac{R_2}{r} = \frac{c(P)}{qr} Q_2 R_2$

* $c(Q_2) = q$ et $c(R_2) = r$

$P = \frac{c(P)}{c(Q_2) c(R_2)} Q_2 R_2$

$c(P) =$

$P = c(P) \frac{Q_2}{c(Q_2)} \cdot \frac{R_2}{c(R_2)}$

$= Q \cdot R$ avec $Q = c(P) \frac{Q_2}{c(Q_2)}$ et $R = \frac{R_2}{c(R_2)}$

donc $P$ est réductible dans $\mathbb{Z}[X]$

car $Q \in \mathbb{Z}[X]$ ($Q_2$ et $R_2 \in \mathbb{Z}[X]$)

En fait, on peut s'arrêter là !

⑤ Montrons l'autre d'existence par l'absurde.

Si $P$ réductible dans $\mathbb{Q}[X]$ alors il l'est dans $\mathbb{Z}[X]$

donc $P = QR$ avec $Q, R \in \mathbb{Z}[X]$

(4) Soit $P \in \mathbb{Z}[X]$. Montrons que $P$ irréductible dans $\mathbb{Q}[X]$
$\Rightarrow P$ irréductible dans $\mathbb{Z}[X]$

Soit $c(P)$ le contenu de $P$.

$P = c(P) P_1$ avec $P_1$ primitif dans $\mathbb{Z}[X]$

Si $P$ est irréductible dans $\mathbb{Q}[X]$ alors $P_1$ aussi.

donc $P_1 = Q_1 R_1$ avec $Q_1, R_1 \in \mathbb{Q}[X]$ non constants

Soit $q$ le produit des dénominateurs des coeffs de $Q_1$ ($\neq 0$)

$r$ ——— ——— ——— de $R_1$ ($\neq 0$)

On introduit ① $\begin{cases} Q_1 = \frac{1}{q} Q_2 \\ R_1 = \frac{1}{r} R_2 \end{cases}$ avec $Q_2, R_2 \in \mathbb{Z}[X]$ par construction

On a donc $Q_2 R_2 = qr\, Q_1 R_1 = qr\, P_1$ ⊛

Passons au contenu : (Étape intermédiaire)

$c(qr P_1) = qr\, \underbrace{c(P_1)}_{=1 \text{ car } P_1 \text{ primitif}} = \boxed{qr \underbrace{=}_{⊛} c(Q_2 R_2)}$ (A)

$= c(Q_2)\, c(R_2)$ d'après 2)

$= q \cdot c(Q_1) \times r \cdot c(R_1)$ d'après ①

$= qr\, c(Q_1)\, c(R_1)$

Or $qr = qr \underbrace{c(Q_1)}_{\in \mathbb{Z}} \underbrace{c(R_1)}_{\in \mathbb{Z}} \Rightarrow c(Q_1) = c(R_1) = 1$

donc d'après ① $\begin{cases} c(Q_2) = q\, c(Q_1) = q \\ c(R_2) = r\, c(R_1) = r \end{cases}$ c'est ce qu'on voulait

On repart de $P$ montrer.

$P = c(P) \cdot P_1 = c(P)\, Q_1 R_1$

$= c(P) \dfrac{Q_2}{\uparrow} \dfrac{R_2}{r} = c(P) \dfrac{Q_2 R_2}{qr} \underset{④}{=} \dfrac{c(P)\, c(Q_2 R_2)}{c(Q_2 R_2)}$

$= c(P) \dfrac{Q_2}{c(Q_2)} \dfrac{R_2}{c(R_2)}$ d'après l'étape intermédiaire

$= \underline{Q} \cdot \underline{R}$ avec $Q = \dfrac{c(P)\, Q_2}{c(Q_2)}$ et $R = \dfrac{R_2}{c(R_2)}$

avec $\dfrac{Q_2}{c(Q_2)} \in \mathbb{Z}[X]$ et $\dfrac{R_2}{c(R_2)} \in \mathbb{Z}[X]$

et donc $c(P) \dfrac{Q_2}{c(Q_2)} \in \mathbb{Z}[X]$ et $\dfrac{R_2}{c(R_2)} \in \mathbb{Z}[X]$

donc $P$ est réductible dans $\mathbb{Z}[X]$.

Donc $P$ réductible dans $\mathbb{Q}[X] \Rightarrow P$ réductible dans $\mathbb{Z}[X]$

par contraposée $P$ irréductible dans $\mathbb{Z}[X] \Rightarrow P$ irréductible dans $\mathbb{Q}[X]$

↑ il y a que ce résultat d'intéressant !

⑤ Critère d'Eisenstein.

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

alors d'après ④, il l'est dans $\mathbb{Z}[X]$

$P = QR$ avec $Q \in \mathbb{Z}[X]$ et $R \in \mathbb{Z}[X]$ avec $\deg Q < n$

$\deg R < n$

Notons $Q(X) = \sum_{k=0}^{q} b_k X^k$ et $R(X) = \sum_{k=0}^{r} c_k X^k$ $\begin{cases} 1 \leq q \leq n-1 \\ 1 \leq r \leq n-1 \end{cases}$

On se place dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\overline{P} = \overline{Q}\,\overline{R}$

d'après la hypothèse sur $P$

$\overline{P} = \overline{p_n} X^n$ car $p \nmid p_n$ et $p \mid p_i$ $\forall i \in [\![0, n-1]\!]$
$\neq 0$

or $\overline{p_n} = \overline{b_q} \cdot \overline{c_r}$ donc $\overline{b_q}$ et $\overline{c_r} \neq 0$ (intègre $\mathbb{Z}/p\mathbb{Z}$)

d'où $\overline{Q}$ est de degré $q$ et $\overline{R}$ de degré $r$.

Par unicité de la décomposition en facteurs irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$

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

tous les coeff sont nuls hormis celui de deg. $n$.

$\Rightarrow \overline{Q}(X) = \overline{b_q} X^q$ et $\overline{R} = \overline{c_r} X^r$

ie les autres coeff $b_i$ et $c_j$ $\forall i \in [\![0, q-1]\!]$
$\forall j \in [\![0, r-1]\!]$

sont divisibles par $p$.

donc en particulier $p \mid b_0$ et $p \mid c_0$

d'où $p^2 \mid b_0 c_0 = a_0$

or d'après l'hypothèse $p^2 \nmid a_0$. contradiction.

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

# Utilisation du critère d'Eisenstein.

Polynômes cyclotomiques.

$p$ premier $\Phi_p(X) = 1 + X + \dots + X^{p-1}$. Rq il est irréductible dans $\mathbb{Z}[X]$

$$\Phi_p(X+1) = \sum_{k=0}^{p-1} (1+X)^k$$

$$= \frac{1-(1+X)^p}{1-(X+1)} \quad \text{(série géom.)}$$

$$= -\frac{1}{X}\left(1 - \sum_{k=0}^{p} \binom{p}{k} X^k\right)$$

$$= -\frac{1}{X}\left(X - X - \sum_{k=1}^{p-1} \binom{p}{k} X^k - X^p\right)$$

$$= -\frac{1}{X}\left(-\sum_{k=1}^{p-1} \binom{p}{k} X^k - X^p\right)$$

$$= \sum_{k=1}^{p-1} \binom{p}{k} X^{k-1} + X^{p-1}$$

$$= \sum_{k=0}^{p-2} \binom{p}{k+1} X^k + X^{p-1}$$

or $p \mid \binom{p}{j}$ et $p^2 \nmid p$ et $p \nmid 1$

donc irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.

Autre polynôme $P(X) = X^n + p$ avec $p$ premier irréductible dans $\mathbb{Z}[X]$