Critère d'Eisenstein

Francinou-Gianella-Nicolas, *Oraux X-ENS Algèbre 1*, page 172

Exercice :

1. (a) On dit qu'un polynôme non nul de $\mathbb{Z}[X]$ est *primitif* si le *pgcd* de ses coefficients est égal à 1. Montrer que le produit de deux polynômes primitifs de $\mathbb{Z}[X]$ est primitif.

   (b) Pour $A \in \mathbb{Z}[X]$ non nul, on appelle *contenu de A*, et on note $c(A)$ le *pgcd* des coefficients de A. Soient A et B deux polynômes non nuls de $\mathbb{Z}[X]$. Montrer que $c(AB) = c(A)c(B)$.

2. Soit $A = a_nX^n + \ldots a_1X + a_0 \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que

$$\begin{array}{cl} (i) & p \text{ ne divise pas } a_0 \\ (ii) & p \text{ divise } a_0, a_1, \ldots, a_{n-1} \\ (iii) & p^2 \text{ ne divise pas } a_0 \end{array}$$

   Montrer que A est irréductible dans $\mathbb{Q}[X]$.

1. (a) Soient $A = \sum\limits_{k=0}^{n} a_kX^k$, $B = \sum\limits_{k=0}^{m} b_kX^k$ des polynômes à coefficients entiers et $C = \sum\limits_{k=0}^{m+n} c_kX^k = AB$. Supposons A et B primitifs et montrons en raisonnant par l'absurde, que C est primitif. Si ce n'est pas le cas, il existe un nombre premier p divisant tous les c_k. Pour $P \in \mathbb{Z}[X]$, notons $\overline{P}$ le projeté de P dans $(\mathbb{Z}/p\mathbb{Z})[X]$: si $P = \sum\limits_{k\in\mathbb{N}} s_kX^k$, $\overline{P} = \sum\limits_{k\in\mathbb{N}} \overline{s_k}X^k$, où $\overline{s_k}$ est la classe de s_k modulo p. Comme p divise tous les c_k, on a $\overline{C} = 0$ et donc $\overline{A}\,\overline{B} = \overline{AB} = \overline{C} = 0$. Mais $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc on a $\overline{A} = 0$ ou $\overline{B} = 0$. Autrement dit, p divise tous les coefficients de A ou tous les coefficients de B. Ceci est exclu.

   On conclut que le produit de deux polynômes primitifs de $\mathbb{Z}[X]$ est encore primitif.

   (b) On peut écrire $AB = c(A)c(B)\dfrac{A}{c(A)}\dfrac{B}{c(B)}$. Alors les polynômes $\dfrac{A}{c(A)}$ et $\dfrac{B}{c(B)}$ sont primitifs, donc leur produit aussi d'après la question précédente, et le contenu de AB est $c(A)c(B)$.

2. Montrons que si A n'est pas irréductible dans $\mathbb{Q}[X]$, alors il peut s'écrire $A = BC$ avec B et C dans $\mathbb{Z}[X]$ de degrés strictement inférieurs à celui de A.

   Soient $\alpha = c(A)$ et $A' = A/\alpha \in \mathbb{Z}[X]$; A' est primitif. A étant composé, par hypothès, A' l'est aussi et on peut écrire $A' = B'C'$, avec B' et C' dans $\mathbb{Q}[X]$ de degrés strictement inférieurs à celui de A. Notons β (resp. γ) le produit des dénominateurs des coefficients de B' (resp. C'). Alors les polynômes $B = \beta B'$ et $C = \gamma C'$ sont dans $\mathbb{Z}[X]$ et $\beta\gamma A' = BC$. En passant aux contenus, on obtient $\beta\gamma = \beta\gamma c(A') = c(B)c(C)$. Par conséquent, on a

$$A = \alpha(B/\beta)(C/\gamma) = \alpha(B/c(B))(C/c(C)) = (\alpha B/c(B))(C/c(C))$$

   et $\alpha B/c(B)$ et $C/c(C)$ sont à coefficients entiers de degré strictement inférieur à celui de A.

   Passons à la démonstration proprement dire du critère d'Eisenstein. Raisonnons par l'absurde et supposons A non irréductible. D'après ce qui précède, il existe B et C dans $\mathbb{Z}[X]$, de degrés strictement inférieurs à n, tels que $A = BC$. Ecrivons $B = b_kX^k + \ldots + b_1X + b_0$ et $C = c_lX^l + \ldots + c_1X + c_0$, avec $k = \deg B$ et $l = \deg C$. Comme dans la question précédente, on projette l'égalité $A = BC$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Il vient $\overline{a_n}X^n = \overline{B}\,\overline{C}$. Les polynômes $\overline{B}$ et $\overline{C}$ sont de degrés respectifs k et l car $b_kc_l = a_n$ n'étant pas divisible par p, $\overline{b_k} \neq 0$ et $\overline{c_l} \neq 0$. Par unicité de la décomposition en irréductibles dans $(\mathbb{Z}/p\mathbb{Z})[X]$, $\overline{B} = \overline{b_k}X^k$ et $\overline{C} = \overline{c_l}X^l$. On a alors $\overline{b_0} = \overline{c_0} = 0$, c'est-à-dire $p|b_0$ et $p|c_0$. Mais alors p^2 divise $a_0 = b_0c_0$ ce qui contredit (iii).

Exemple : $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ pour tout entier $n \geq 1$ (prendre $p = 2$), ce qui prouve qu'il y a dans $\mathbb{Q}[X]$ des irréductibles de tout degré.