CONTENU D'UN POLYNÔME ET CRITÈRE D'EISENSTEIN

On appelle contenu d'un polynôme non-nul $R \in \mathbb{Z}[X]$ et on note $c(R)$ le PGCD de ses coefficients. Soient A et B deux polynômes non-nuls et P un polynôme non-constant de $\mathbb{Z}[X]$.

1. ***Prouver que si $c(A) = c(B) = 1$ alors $c(AB) = 1$.***
2. ***Prouver que $c(AB) = c(A)c(B)$.***
3. ***En déduire que P est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il l'est dans $\mathbb{Q}[X]$.***

On pose $A = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ où $n \in \mathbb{N}^*$. On suppose qu'il existe un nombre premier p tel que :

i. ***p ne divise pas a_n***
ii. ***p divise a_k pour $0 \leq k \leq n-1$***
iii. ***p^2 ne divise pas a_0***

4. ***Prouver que A est irréductible dans $\mathbb{Q}[X]$.***

---

1. ***Prouver que si $c(A) = c(B) = 1$ alors $c(AB) = 1$.***

Procédons par l'absurde et supposons que $c(A) = c(B) = 1$ mais que $c(AB) \neq 1$.

Alors il existe un nombre premier p tel que p divise tous les coefficients de AB, de sorte que dans $\mathbb{Z}/p\mathbb{Z}$ on a : $\overline{AB} = \overline{0}$.

Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est intègre donc $\mathbb{Z}/p\mathbb{Z}[X]$ l'est aussi, d'où : $\bar{A} = \overline{0}$ ou $\bar{B} = \overline{0}$. Supposons par exemple que $\bar{A} = \overline{0}$, c'est à dire que :

$$\overline{\sum_{k=0}^{n} a_k X^k} = \sum_{k=0}^{n} \overline{a_k X^k} = \sum_{k=0}^{n} \overline{a_k} X^k = \overline{0}$$

Ainsi, pour tout $k \in [\![0; n]\!]$, $\overline{a_k} = \overline{0}$. Autrement dit, p diviser tous les coefficients de A, ce qui contredit $c(A) = 1$. On procède de même si $\bar{B} = \overline{0}$.

Cette contradiction assure que $c(AB) = 1$.

2. ***Prouver que $c(AB) = c(A)c(B)$.***

On pose $A = c(A)A_1$ et $B = c(B)B_1$ de sorte que A_1 et B_1 soient de contenu 1. Alors :

$c(AB) = c(c(A)A_1 c(B)B_1) = c(A)c(B)c(A_1B_1) = c(A)c(B)$ car $c(A_1B_1) = 1$ d'après la question 1.

3. ***En déduire que P est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il l'est dans $\mathbb{Q}[X]$.***

Si P est irréductible dans $\mathbb{Q}[X]$ il l'est évidemment dans $\mathbb{Z}[X]$.

Il reste à montrer que si P est irréductible dans $\mathbb{Z}[X]$ alors il l'est aussi dans $\mathbb{Q}[X]$. Supposons que ce n'est pas le cas et que $P = AB$ où A et B sont dans $\mathbb{Q}[X]$.

Notons m le produit des dénominateurs des coefficients de A et de B. Alors $A_1 = mA$ et $B_1 = mB$ sont dans $\mathbb{Z}[X]$ d'où :

$$m^2P = A_1B_1$$

$$m^2P = c(A_1)A_2c(B_1)B_2$$

où A_2 et B_2 sont dans $\mathbb{Z}[X]$ tels que $c(A_2) = c(B_2) = 1$

$$m^2\, c(P) = c(A_1)c(B_1)c(A_2B_2) = c(A_1)c(B_1)$$

Des deux dernières lignes, on tire : $m^2P = m^2c(P)A_2B_2$ c'est à dire $P = c(P)A_2B_2$

ce qui contredit le caractère irréductible de P dans $\mathbb{Z}[X]$. On peut conclure que P est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il l'est dans $\mathbb{Q}[X]$.

On pose $A = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ où $n \in \mathbb{N}^*$. On suppose qu'il existe un nombre premier p tel que :

i. ***p ne divise pas a_n***
ii. ***p divise a_k pour $0 \leq k \leq n-1$***
iii. ***p^2 ne divise pas a_0***

4. ***Prouver que A est irréductible dans $\mathbb{Q}[X]$.***

On suppose par l'absurde que $A = BC$ où $B = \sum_{k=0}^{r} b_kX^k$, $C = \sum_{k=0}^{s} c_kX^k$, $b_rc_s = b_k$, $b_0c_0 = a_0$. Nous avons vu qu'il suffit de prouver la propriété dans $\mathbb{Z}[X]$.

- Raisonnons sur les coefficients dominants dans $\mathbb{Z}/p\mathbb{Z}$:

  $\overline{b_r}\overline{c_s} = \overline{b_k} \neq \overline{0}$ donc $\overline{b_r}$ et $\overline{c_s}$ ne peuvent pas être nuls.

- Raisonnons sur les coefficients constants dans $\mathbb{Z}/p\mathbb{Z}$:

  p divise a_0 donc $\overline{b_0}\overline{c_0} = \overline{a_0} = \overline{0}$ et comme $\mathbb{Z}/p\mathbb{Z}$ est intègre, $\overline{b_0} = \overline{0}$ ou $\overline{c_0} = \overline{0}$ mais pas les deux sinon p^2 diviserait $b_0c_0 = a_0$ ce qui est contraire aux hypothèses sur p.

Supposons par exemple que $\overline{b_0} = \overline{0}$ et $\overline{c_0} \neq \overline{0}$ alors $\bar{B}$ est de la forme $\overline{b_r}X^r + \cdots + \overline{b_t}X^t$ où $t \geq 1$. Alors $\bar{A} = \overline{b_r}\overline{c_s}X^{r+s} + \cdots + \overline{b_t}\overline{c_0}X^t$ avec $\overline{b_t}\overline{c_0} \neq \overline{0}$ donc le $t^{ième}$ coefficient de $\bar{A}$ est non-nul. Or, seul le coefficient dominant est non-nul dans $\mathbb{Z}/p\mathbb{Z}$ mais $t \leq r < n$. C'est absurde.

Le critère d'Eisenstein permet donc d'affirmer que P est irréductible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$.