

Devoir Libre n° 15

Contenu d'un polynôme et critère d'Eisenstein

1. Si a_0, \dots, a_n sont les coefficients de P ,

$$c(kP) = \bigwedge (ka_i) = |k| \bigwedge a_i = |k| c(P)$$

et donc $c(kP) = |k|c(P)$.

2.a) Pour tout $i \in \llbracket 0, n+m \rrbracket$, $c_i = \sum_{k=0}^i a_k b_{i-k}$.

2.b) Si $\mathcal{A} \neq \emptyset$ et $\mathcal{B} \neq \emptyset$, alors comme ce sont des parties de \mathbb{N} , elles admettent des minima k_0 et ℓ_0 et $p \mid c_{k_0+\ell_0} = \sum_{k=0}^{k_0+\ell_0} a_k b_{k_0+\ell_0-k}$ par hypothèse. Or si $k \notin \mathcal{A}$, comme p est premier, $p \mid a_k$, donc en particulier si $k < k_0$, $p \mid a_k$. De même, si $\ell < \ell_0$, $p \mid b_\ell$, donc si $k > k_0$, $p \mid b_{k_0+\ell_0-k}$. On a alors que $p \mid a_{k_0} b_{\ell_0}$ donc, comme il est premier, p divise soit a_{k_0} soit b_{ℓ_0} ce qui est en contradiction avec le fait que $k_0 \in \mathcal{A}$ et $\ell_0 \in \mathcal{B}$. Ainsi, $\mathcal{A} = \emptyset$ ou $\mathcal{B} = \emptyset$.

2.c) Ainsi et toujours parce que p est premier, on a bien

soit p divise tous les coefficients de A , soit p divise tous les coefficients de B .

3. Si $c(AB) \neq 1$, il a un diviseur premier p , donc p divise tous les coefficients de AB et donc par la question précédente, tous les coefficients de A ou de B et donc, soit $c(A)$, soit $c(B)$.

Ainsi, par contraposée, si A et B sont primitifs, AB l'est.

4. Si a_0, \dots, a_n sont les coefficients de A et b_0, \dots, b_m sont les coefficients de B , alors on a a'_0, \dots, a'_n premiers entre eux dans leur ensemble tels que pour tout i , $a_i = c(A)a'_i$ et b'_0, \dots, b'_m premiers entre eux dans leur ensemble tels que pour tout i , $b_i = c(B)b'_i$.

Ainsi, $\frac{1}{c(A)}A$ et $\frac{1}{c(B)}B$ sont primitifs.

D'après la question précédente, $\frac{AB}{c(A)c(B)}$ est aussi primitif, donc $c\left(\frac{AB}{c(A)c(B)}\right) = 1$. Or, d'après la première question,

$$c(AB) = c\left(c(A)c(B)\frac{AB}{c(A)c(B)}\right) = c(A)c(B)\left(\frac{AB}{c(A)c(B)}\right) = c(A)c(B)$$

(un contenu est toujours positif).

Ainsi $c(AB) = c(A)c(B)$.

5.a) Comme A et B sont non nuls, on peut poser k_1 égal au ppcm des coefficients de A et k_2 égal au ppcm des coefficients de B . Alors, en mettant au même dénominateur les coefficients, on a bien $A_1, B_1 \in \mathbb{Z}[X]$ tels que $P = \frac{1}{k_1 k_2} A_1 B_1$.

5.b) On a alors $k_1 k_2 P = A_1 B_1$ avec $k_1 k_2 \geq 0$ donc $k_1 k_2 c(P) = c(A_1 B_1) = c(A_1) c(B_1)$ d'après les questions 1 et 4.

Soit $r = \frac{k_1}{c(B_1)} \in \mathbb{Q}^*$. Alors $r = k_1 \frac{B_1}{c(B_1)} \in \mathbb{Z}[X]$ et $\frac{1}{r} = \frac{k_2}{c(B_2)}$ est tel que $\frac{1}{r} B = k_2 \frac{B_2}{c(B_2)} \in \mathbb{Z}[X]$.

6. Si, par contraposée, $P \in \mathbb{Z}[X] \setminus \{0\}$ est réductible dans $\mathbb{Q}[X]$, soit P est constant, soit on a $A, B \in \mathbb{Q}[X]$ non constants tels que $\frac{P}{c(P)} = AB$. D'après la question précédente, on a $r \in \mathbb{Q}$ tel que $A_2 = \frac{1}{r}A, B_2 = rB \in \mathbb{Z}[X]$ et sont non constant. Alors $P = c(P)A_2 B_2$ et P est réductible dans $\mathbb{Z}[X]$.

Donc si P est irréductible dans $\mathbb{Z}[X]$, il l'est dans $\mathbb{Q}[X]$.

7.a) Si $P = AB$ avec $A, B \in \mathbb{Z}[X]$, notons m le degré de $A = a_0 + a_1 X + \dots + a_{m-1} X^{m-1} + a_m X^m$. Ensuite, $p \mid c_0 = a_0 b_0$ donc $p \mid a_0$ ou $p \mid b_0$. On suppose par exemple que $p \mid a_0$. Comme $p^2 \nmid c_0$, on a alors $p \nmid b_0$.

On a ensuite $p \mid c_1 - a_0 b_1 = a_1 b_0$ et donc $p \mid a_1 b_0$, mais comme $p \nmid b_0$ (et p premier), $p \mid a_1$. Si, par récurrence, p divise a_0, \dots, a_{k-1} , avec $k \in \llbracket 1, m \rrbracket$, alors

$$p \mid c_k - (a_0 b_k + a_1 b_{k-1} + \dots + a_{k-1} b_1) = a_k b_0$$

donc $p \mid a_k b_0$ et donc $p \mid a_k$, ce qui établit la récurrence. Ainsi, p divise tous les coefficients de A .

Par symétrie, on a bien p divise tous les coefficients de A ou de B .

7.b) D'après 6, il suffit de montrer que P est irréductible dans $\mathbb{Z}[X]$. Or si P est réductible et non constant dans $\mathbb{Z}[X]$, on a $A, B \in \mathbb{Z}[X]$ non constants tels que $P = AB$. D'après la question précédente, p divise tous les coefficients de A ou de B . Or $1 = cd(P) = cd(A)cd(B)$ donc $cd(A) = cd(B) = \pm 1$ car entiers. C'est contradictoire.

Ainsi, P est irréductible sur \mathbb{Q} .

8. Pour $P = X^5 - 2$ et $Q = X^4 + 2X^2 + 2X + 2$, P et Q vérifient bien la propriété précédente avec $p = 2$, donc sont irréductibles sur \mathbb{Q} .