Partie 1 : Contenu d'un polynôme à coefficients entiers

1. a. Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ non nul et $k \in \mathbb{N}^*$. Par linéarité (ou homogénéité) :

$$\operatorname{pgcd}(ka_0, ..., ka_n) = k \operatorname{pgcd}(a_0, ..., a_n).$$

De $kp = \sum_{i=0}^{n} ka_i X^i$, on tire

$$c(kP) = \operatorname{pgcd}(ka_0, ..., ka_n) = k \operatorname{pgcd}(a_0, ..., a_n) = kc(P).$$

b. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ non nul, de degré n et de coefficients $a_0, ..., a_n$.
Pour tout $k \in [\![0, n]\!]$, $c(P)$ divise a_k donc il existe $a'_k \in \mathbb{Z}$ tel que $a_k = c(P)a'_k$.
Ainsi :

$$\frac{1}{c(P)} P = \sum_{k=0}^{n} a'_k X^k \in \mathbb{Z}[X].$$

2. Soit $k \in [\![0, n+m]\!]$. Par définition du produit polynomial :

$$c_k = \sum_{\substack{(i,j) \in [\![0,n]\!] \times [\![0,m]\!] \\ i+j=k}} a_i b_j.$$

3. a. Comme $c(A) = c(B) = 1$, les coefficients de A n'ont aucun diviseur commun donc p ne divise pas tous les a_i et il en est de même pour les coefficients de B. Les ensembles d'indices i pour lesquels p ne divise pas a_i ou b_i sont des parties de $\mathbb{N}$ *non vides*. Elles admettent des plus petits éléments. Les entiers k_0 (associé à A) et l_0 (associé à B) sont donc bien définis.

b. D'après la question 2., on a :

$$c_{k_0+l_0} = \sum_{\substack{(i,j) \in [\![0,n]\!] \times [\![0,m]\!] \\ i+j=k_0+l_0}} a_i b_j = a_{k_0} b_{l_0} + \sum_{\substack{(i,j) \in [\![0,n]\!] \times [\![0,m]\!] \\ i+j=k_0+l_0 \\ (i,j) \neq (k_0,l_0)}} a_i b_j$$

Examinons les couples (i, j) de la dernière somme.
Montrons d'abord que $i \neq k_0$ et $j \neq l_0$. En effet

$$\left.\begin{array}{r} i = k_0 \\ i + j = k_0 + l_0 \end{array}\right\} \Rightarrow j = l_0 \Rightarrow (i, j) = (k_0, l_0).$$

De même pour $j = l_0$. Montrons ensuite que $i < k_0$ ou $j < l_0$. En effet

$$\left.\begin{array}{r} i \geq k_0 \\ i \neq k_0 \\ i + j = k_0 + l_0 \end{array}\right\} \Rightarrow \left.\begin{array}{c} i < k_0 \\ i + j = k_0 + l_0 \end{array}\right\} \Rightarrow j > l_0.$$

De même $j \geq l_0$ entraîne $i < k_0$.
Ainsi, p divise a_i ou b_j, donc dans tous les cas, p divise $a_i b_j$.
La somme :

$$\sum_{\substack{(i,j) \in [\![0,n]\!] \times [\![0,m]\!] \setminus \{(k_0,l_0)\} \\ i+j=k_0+l_0}} a_i b_j = c_{k_0+l_0} - a_{k_0} b_{l_0}$$

est donc divisible par p. De $c_{k_0+l_0}$ divisible par p, on déduit que $a_{k_0} b_{l_0}$ l'est aussi.

c. Comme p divise $a_{k_0} b_{l_0}$ avec p premier, le lemme de Gauss assure que p divise a_{k_0} ou b_{l_0}, ce qui contredit la définition de k_0 et de l_0. C'est donc absurde.
Ainsi, $c(AB)$ ne possède pas de diviseurs premiers, donc $c(AB) = 1$.

4. Notons $p = c(A)$, $q = c(B)$. Pour tout $k \in [\![0, n]\!]$ et tout $l \in [\![0, m]\!]$, il existe a'_k et b'_l entiers tels que $pa'_k = a_k$ et $qb'_l = b_l$.
Par linéarité, $\operatorname{pgcd}(a'_0, ..., a'_n) = \operatorname{pgcd}(b'_0, ..., b'_m) = 1$. Ainsi :

$$A_1 = \sum_{k=0}^{n} a'_k X^k \text{ et } B_1 = \sum_{l=0}^{m} b'_l X^l \text{ vérifient } c(A_1) = c(B_1) = 1.$$

Donc $c(A_1 B_1) = 1$ d'après 3.c.. Comme $AB = pqA_1 B_1$, la question 1.a. entraîne :

$$c(AB) = pq\, c(A_1 B_1) = pq = c(A)c(B).$$

5. a. Notons $u = \deg(Q)$. Comme $Q \in \mathbb{Q}[X]$, il existe $(p_0, ..., p_u) \in \mathbb{Z}^{u+1}$ et $(q_0, ..., q_{u+1}) \in (\mathbb{N}^*)^{n+1}$ tels que :

$$Q = \sum_{k=0}^{u} \frac{p_k}{q_k} X^k.$$

Posons alors $q = \operatorname{ppcm}(q_0, ..., q_u)$. Pour tout $k \in [\![0, u]\!]$, q_k divise q donc :

$$q \frac{p_k}{q_k} \in \mathbb{Z}.$$

Ainsi, $qQ \in \mathbb{Z}[X]$. De même, on trouve un entier naturel r tel que $rR \in \mathbb{Z}[X]$.

b. D'après les hypothèses sur $P \in \mathbb{Z}[X]$ et Q, R dans $\mathbb{Q}[X]$,

$$P = QR \Rightarrow qrQR = qrP \Rightarrow c(qrQR) = c(qrP) = qrc(P) \Rightarrow qr \text{ divise } c(qrQR)$$

c. Définissons plusieurs polynômes de $\mathbb{Z}[X]$ (question a. et définition du contenu) :

$$S_1 = qQ, \quad T_1 = rR, \quad S_2 = \frac{1}{c(S_1)} S_1, \quad T = \frac{1}{c(T_1)} T_1$$

Alors : $c(S_1)c(T_1) = c(S_1T_1) = c(qr\,QR) = qr\,c(P)$. On en déduit

$$P = \frac{1}{qr}(qQ)(rR) = \frac{1}{qr}S_1T_1 = \frac{c(S_1)c(T_1)}{qr}S_2T = \underbrace{c(P)\,S_2}_{=S\in\mathbb{Z}[X]}\,T$$

On a donc bien : $P = ST$ avec P et Q à coefficients entiers et de degrés non nuls.

Partie 2 : Critère d'Eisenstein

1. a. On a $a_0 = b_0c_0$. Comme p divise a_0 et p est premier, d'après le lemme d'Euclide, p divise b_0 ou p divise c_0.
Comme p^2 ne divise pas a_0, alors p ne peut diviser simultanément b_0 et c_0. Donc p divise exactement l'un des deux entiers b_0 et c_0.

b. Montrons le résultat par récurrence finie sur k. Pour tout $k \in [\![0, r]\!]$, notons P_k la proposition :

$$P_k : \quad \forall l \in [\![0, k]\!],\ p \text{ divise } b_l$$

- P_0. C'est ce que nous avons supposé dans la question précédente.
- $P_k \Rightarrow P_{k+1}$. Soit $k \in [\![0, r-1]\!]$ tel que P_k soit vérifiée. Comme $s \geq 1$, alors $r < n$ donc $k+1 < n$. Ainsi, p divise a_{k+1}. On a :

$$a_{k+1} = \sum_{\substack{0\leq i\leq r\\ 0\leq j\leq s\\ i+j=k+1}} b_ic_j = b_{k+1}c_0 + \sum_{\substack{0\leq i\leq r,\ i\neq k+1\\ 0\leq j\leq s\\ i+j=k+1}} b_ic_j.$$

Soit $(i, j) \in [\![1, r]\!] \times [\![0, s]\!]$ tel que $i + j = k + 1$ et $i \neq k + 1$. Alors $i \leq k$. D'après P_k, p divise b_i. Ainsi, p divise la somme :

$$\sum_{\substack{0\leq i\leq r,\ i\neq k+1\\ 0\leq j\leq s\\ i+j=k+1}} b_ic_j.$$

Comme p divise a_{k+1}, alors p divise $b_{k+1}c_0$. D'après le lemme d'Euclide, p divise b_{k+1} ou c_0. Comme p ne divise pas c_0, alors p divise b_{k+1}.
Donc P_{k+1} est vérifiée.
Conclusion : $\forall k \in [\![0, r]\!]$, $p|b_k$.

c. Ainsi, p divise b_r. Or, $a_n = b_rc_s$, donc p divise a_n. Ceci est absurde, puisque d'après l'hypothèse (ii), p ne divie pas a_n.
On en déduit que'il n'existe pas de polynômes $B, C \in \mathbb{Z}[X]$ de degrés supérieurs ou égaux à 1 tels que $A = BC$.

2. D'après la question **5.c.**, P est irréductible dans $\mathbb{Q}[X]$.

Partie 3 : Exemples

1. Posons $a_0 = -2$, $a_1 = ... = a_{n-1} = 0$ et $a_n = 1$. Posons également $p = 2$. On a bien :

$$p \text{ divise } a_0, \cdots, a_{n-1}, \quad p \text{ ne divise pas } a_n, \quad p^2 = 4 \text{ ne divise pas } a_0 = -2.$$

D'après le critère d'Eisenstein (question 7.), $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$.

2. a. D'après les règles de calcul dans un anneau :

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

b. On substitue $X + 1$ à X dans la relation précédente puis on simplifie par X

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

$$\Rightarrow \Psi_p = \sum_{k=0}^{p-1}\binom{p}{k+1}X^k.$$

c. Pour tout $k \in [\![0, p-1]\!]$, posons $a_k = \binom{p}{k+1}$.
Pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$ (voir démonstration du petit théorème de Fermat), donc pour tout $k \in [\![0, p-2]\!]$, p divise a_k. De plus,

$$a_{p-1} = 1 \Rightarrow p \text{ ne divise pas } a_{p-1}, \qquad a_0 = p \Rightarrow p^2 \text{ ne divise pas } a_0.$$

D'après le critère d'Eisenstein (question 7.), Ψ_p est irréductible dans $\mathbb{Q}[X]$.

d. Montrons par l'absurde que Φ_p est irréductible dans $\mathbb{Q}[X]$.
S'il existe $A, B \in \mathbb{Q}[X]$ avec $\deg(A), \deg(B) \geq 1$ tels que $\Phi_p = AB$. Alors en substituant $X+1$ à X :

$$\Psi_p = \widehat{A}(X+1)\,\widehat{B}(X+1)$$

ne serait pas irréductible, en contradiction avec le résultat de la question précédente. Le polynôme Φ_p est bien irréductible dans $\mathbb{Q}[X]$.