POLYNÔMES IRRÉDUCTIBLES DANS $\mathbb{Q}[X]$

Dans tout ce problème $\mathbb{Q}[X]$ (respectivement $\mathbb{Z}[X]$) désigne l'ensemble des polynômes à une indéterminée, à coefficients dans $\mathbb{Q}$ (respectivement $\mathbb{Z}$). Ces ensembles sont des anneaux commutatifs pour les lois $+$ et $\times$ usuelles sur les polynômes.
Un polynôme Φ de $\mathbb{Q}[X]$ (respectivement $\mathbb{Z}[X]$) est dit irréductible sur $\mathbb{Q}$ (respectivement $\mathbb{Z}$) s'il n'est ni constant, ni de la forme $\Phi = PQ$ avec P, Q dans $\mathbb{Q}[X]$ (respectivement $\mathbb{Z}[X]$) et $\deg(P) \geqslant 1$, $\deg(Q) \geqslant 1$.

Partie I: Exemples.

1. Montrer que les polynômes $X^2 - X - 1$ et $X^3 - X - 1$ sont irréductibles sur $\mathbb{Z}$.
2. Soit $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n$ des entiers relatifs deux à deux distincts. Définissons Φ par
$$\Phi = (X - a_1) \ldots (X - a_n) - 1$$
On remarque que $\Phi \in \mathbb{Z}[X]$. Le but de la question est de montrer qu'il est irréductible sur $\mathbb{Z}$. Supposons qu'il existe P et Q dans $\mathbb{Z}[X]$ de degré supérieur ou égal à 1 et vérifiant $\Phi = PQ$.
   (a) Montrer que $a_1, \ldots, a_n$ sont des racines de $P + Q$.
   (b) En déduire que $\Phi = -P^2$.
   (c) Conclure.
3. Soit n un entier naturel impair et soient $a_1, \ldots, a_n$ des entiers relatifs deux à deux distincts. Montrer que $(X - a_1) \ldots (X - a_n) + 1$ est irréductible dans $\mathbb{Z}$.

Partie II: Lemme de Gauss.

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme non nul de $\mathbb{Z}[X]$. On définit le contenu de P, noté $c(P)$ par
$$c(P) = \text{pgcd}(a_0, \ldots, a_n)$$
Le polynôme P est dit primitif si $c(P) = 1$.
Soient P et Q dans $\mathbb{Z}[X]$.

4. On suppose dans cette question que P et Q sont primitifs.
Notons $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{m} b_k X^k$ et $PQ = \sum_{k=0}^{r} c_k X^k$.
Soit p un nombre premier.
   (a) Montrer qu'il existe un plus petit entier $k \in [\![0, n]\!]$ tel que p ne divise pas a_k. Notons le k_0.
   Notons, de même, k_1 le plus petit entier $k \in [\![0, m]\!]$ tel que p ne divise pas b_k.
   (b) Montrer que p ne divise pas $c_{k_0+k_1}$
   (c) En déduire que $c(PQ) = 1$.
5. Montrer que $c(PQ) = c(P)c(Q)$ (lemme de Gauss).

Partie III: Critère d'Eisenstein.

6. Soit $\Phi \in \mathbb{Z}[X]$ pour lequel il existe des polynômes P et Q de degré supérieur ou égal à 1 et à coefficients rationnels tels que $\Phi = PQ$. Montrer qu'il existe deux polynômes P_0 et Q_0 de $\mathbb{Z}[X]$ proportionnels respectivement à P et Q et tels que $\Phi = P_0 Q_0$.
7. Soit $\Phi \in \mathbb{Z}[X]$. Montrer que Φ est irréductible sur $\mathbb{Q}$ si et seulement si il est irréductible sur $\mathbb{Z}$.
8. Soit $\Phi = \sum_{k=0}^{n} a_k X^k$ un polynôme non constant de $\mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que :
   - p ne divise pas a_n
   - p divise a_i pour $i \in \{0, \ldots, n-1\}$
   - p^2 ne divise pas a_0

   Montrer que Φ est irréductible sur $\mathbb{Q}$.

Polynômes irréductibles dans $\mathbb{Q}[X]$

Partie I: Exemples.

1. Supposons qu'il existe a, b, a', b' dans $\mathbb{Z}$ tels que

$$P_1 = X^2 - X - 1 = (aX + b)(a'X + b')$$

Alors, $aa' = 1$ et $bb' = 1$ d'où $a = \pm 1$ et $b = \pm 1$. Le polynôme P_1 devrait donc admettre 1 ou -1 comme racine en contradiction avec $P_1(-1) = 1$ et $P_1(1) = -1$. On en déduit que P_1 est irréductible.
Supposons qu'il existe a, b, a', b', c' dans $\mathbb{Z}$ tels que

$$P_2 = X^3 - X - 1 = (aX + b)(a'X^2 + b'X + c')$$

(le polynôme $a'X^2 + b'X + c'$ étant éventuellement réductible sur $\mathbb{Z}$). Alors $aa' = 1$ et $bc' = 1$ puis $a = \pm 1$ et $b = \pm 1$, et 1 ou -1 serait racine de P_2 en contradiction avec $P_2(-1) = -1$ et $P_2(1) = -1$. On en déduit que P_2 est irréductible.

2. (a) Pour k entre 1 et n, $\Phi(a_k) = P(a_k)Q(a_k) = -1$ d'où $P(a_k) = -Q(a_k) = \pm 1$. On en déduit que $P(a_k) + Q(a_k) = 0$. Les a_k, sont donc des racines de $P + Q$.

   (b) On sait que $\deg(\Phi) = n$ et, par hypothèse, $\deg(P) \geqslant 1$ et $\deg(Q) \geqslant 1$. D'où $\deg(P) \leqslant n-1$ et $\deg(Q) \leqslant n-1$, ainsi $P + Q$ est de degré inférieur ou égal à $n - 1$ tout en admettant au moins n racines. Il est donc nul d'où $Q = -P$ et $\Phi = -P^2$.

   (c) Pour tout $x \in \mathbb{R}$, $\Phi(x) = -(P(x))^2 \leqslant 0$. Or $\lim_{+\infty} \Phi = +\infty$. C'est absurde, le polynôme Φ étant non constant, il est donc irréductible sur $\mathbb{Z}$.

3. Supposons que $\Phi_2 = (X - a_1) \dots (X - a_n) + 1$ soit réductible sur $\mathbb{Z}$.
Ce polynôme étant non constant il s'écrit donc $\Phi_2 = PQ$ avec P et Q dans $\mathbb{Z}[X]$ et de degré supérieur ou égal à 1. On en déduit que P et Q sont de degré inférieur ou égal à $n - 1$.
Comme dans la question précédente, on a, pour k entre 1 et n,

$$\Phi(a_k) = P(a_k)Q(a_k) = 1 \Rightarrow P(a_k) = Q(a_k) = \pm 1$$

On en déduit que $P(a_k) - Q(a_k) = 0$. Les a_k sont donc des racines de $P - Q$ qui est de degré au plus $n - 1$. C'est donc le polynôme nul, d'où $\Phi = P^2$.
On peut alors écrire

$$\prod_{k=1}^{n} (X - a_k) = P^2 - 1 = (P - 1)(P + 1)$$

Comme P n'est pas constant, $\deg(P-1) = \deg(P+1) = \deg(P)$. On devrait alors avoir $n = \deg(P^2-1) = 2 \deg P$ en contradiction avec n impair. On en déduit que le polynôme $(X - a_1) \dots (X - a_n) + 1$ est irréductible sur $\mathbb{Z}$.

Partie II: Lemme de Gauss.

4. (a) Le polynôme P est primitif, donc p ne divise pas le pgcd de $(a_0, \dots, a_n)$. Il existe donc un entier $k \in \{0, \dots, n\}$ tel que p ne divise pas a_k. L'ensemble des k entiers entre 0 et n tels que p ne divise pas a_k est une partie non vide de $\mathbb{N}$, elle admet un plus petit élément.

   (b) Notons k_0 le plus petit des k tels que p ne divise pas a_k et k_1 le plus petit des k tels que p ne divise pas b_k. Considérons le terme de degré $k_0 + k_1$ dans le produit.

$$c_{k_0+k_1} = \sum_{k=0}^{k_0-1} a_k b_{k_0+k_1-k} + a_{k_0} k_{k_1} + \sum_{k=k_0+1}^{k_0+k_1} a_k b_{k_0+k_1-k}$$

   Pour $0 \leqslant k \leqslant k_0 - 1$, p ne divise pas a_k par définition de k_0. Donc p divise la somme de gauche.
   Pour $k_0 + 1 \leqslant k \leqslant k_0 + k_1$, on a $k_0 + k_1 - k < k_1$, donc p divise b_k par définition de k_1. On en déduit que p divise la somme de droite.
   Or p ne divise pas a_{k_0} et p ne divise pas b_{k_1}. Comme il est premier, il ne divise pas leur produit. On en déduit que p ne divise pas $c_{k_0+k_1}$.

(c) Le contenu $c(PQ)$ est un entier naturel qui n'admet aucun diviseur premier. Il est donc égal à 1.

5. Soient P et Q dans $\mathbb{Z}[X]$. Notons $a_0, \cdots, a_n$ les coefficients de P. On peut factoriser le contenu $c(P)$ dans ces coefficients, soit

$$\forall k \in \{0, \ldots, n\}, a_k = c(P)a'_k \qquad \text{et } P_1 = \sum_{k=0}^{n} a'_k X^k$$

avec les a'_k dans $\mathbb{Z}$ et $\text{pgcd}(a'_0, \ldots, a'_n) = 1$. Alors $P = c(P)P_1$ avec $P_1 \in \mathbb{Z}[X]$ polynôme primitif.
De même $Q = c(Q)Q_1$ avec $Q_1 \in \mathbb{Z}[X]$ polynôme primitif.
Par homogénéité du pgcd, $c(PQ) = c(P)c(Q)c(P_1Q_1)$, d'où, par la question précédente, $c(PQ) = c(P)c(Q)$.

Partie III: Critère d'Eisenstein.

6. Notons a (respectivement b) le ppcm des dénominateurs des coefficients de P (respectivement Q) écrits sous forme de fractions irréductibles. Alors $P_1 = aP \in \mathbb{Z}[X]$, $Q_1 = bQ \in \mathbb{Z}[X]$ et $ab\Phi = P_1Q_1$.
Par le lemme de Gauss $ab|c(ab\Phi) = c(P_1)c(Q_1)$. Soit m l'entier relatif tel que $c(P_1)c(Q_1) = abm$.
Introduisons P_2 et Q_2 les polynômes primitifs de $\mathbb{Z}[X]$ tels que $P_1 = c(P_1)P_2$ et $Q_1 = c(Q_1)Q_2$. Alors $\Phi = P_0Q_0$ en prenant $P_0 = mP_2$ et $Q_0 = Q_2$.

7. Le sens direct est évident. Le sens réciproque est conséquence de la question précédente.

8. D'après la question précédente, il suffit de montrer que Φ est irréductible sur $\mathbb{Z}$.
Supposons le contraire. Φ n'étant pas constant, Φ s'écrit donc $\Phi = PQ$ avec P, Q dans $\mathbb{Z}[X]$ et $m = \deg(P) \geqslant 1$, $r = \deg(Q) \geqslant 1$.
Notons $P = \sum_{k=0}^{m} b_k X^k$ et $Q = \sum_{k=0}^{r} c_k X^k$.
On peut remarquer que $a_n \neq 0$ car par hypothèse $p \not| a_n$. D'où $n = \deg(\Phi)$ et $n = m + r$.
Par hypothèse $p|a_0 = b_0c_0$ et $p^2 \not| a_0 = b_0c_0$, donc p divise un et un seul des facteurs. On peut supposer que $p|b_0$.
Notons k le plus petit entier de $\{1, \ldots, m\}$ tel que $p \not| b_k$. Un tel entier existe bien car $p \not| a_n = b_mc_r$, donc $p \not| b_m$.
Alors $a_k = b_kc_0 + \sum_{i=1}^{k} b_{k-i}c_i$. On sait que $k \leqslant m$ et $r \geqslant 1$ donc $k < n = m + r$ donc $p|a_k$.
Or $p|\sum_{i=1}^{k} b_{k-i}c_i$ par définition de k et $p \not| b_k$ et $p \not| c_0$. C'est absurde, donc Φ est irréductible sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$.