THEOREME D'EISENSTEIN

Théorème: Soit $R \in A[X]$ avec A un anneau factoriel. On écrit $R(X) = \sum_{k=0}^{n} a_k X^k$ et $K := \mathrm{Frac}(A)$.
On suppose qu'il existe $p \in A$, premier, satisfaisant les conditions:

(i) $p \mid a_k$, $k = 0, 1, \dots, n-1$

(ii) $p \nmid a_n$

(iii) $p^2 \nmid a_0$

Alors, R est irréductible dans $K[X]$ (et dans $A[X]$ si R est primitif).

Lemme 1: $\forall P, Q \in A[X]$, $c(PQ) = c(P)c(Q)$

Preuve 1: Soit $R = PQ$. Commençons par prouver le lemme dans le cas $c(P) = c(Q) = 1$. Supposons par l'absurde que $c(R) \neq 1$. Alors $\exists p \in A$ irréductible tq. p divise les coeffs de P. En projetant l'égalité $R = PQ$ dans $A/\langle p \rangle [X]$:

$$\bar{R} = \bar{P}\bar{Q} = \bar{0}.$$

Or, comme p est irréductible, $\langle p \rangle$ est premier donc $A/\langle p \rangle$ est intègre, de même que $A/\langle p \rangle [X]$. Ainsi, $\bar{P} = 0$ ou $\bar{Q} = 0$, ce qui est contraire à l'hypothèse $c(P) = c(Q) = 1$.
Donc, $c(R) = 1$. Dans le cas où $c(P) \neq 1$ ou $c(Q) \neq 1$, alors, on écrit:

$$R = PQ = c(P)c(Q)\,\frac{P}{c(P)}\,\frac{Q}{c(Q)}$$

de sorte que $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$ soient primitifs. Donc,

$$\begin{aligned} c(R) &= c(PQ) \\ &= c(P)c(Q)\,c\left(\frac{P}{c(P)} \cdot \frac{Q}{c(Q)}\right) \quad \text{(homogénéité du pgcd)} \\ &= c(P)c(Q) \times 1 \quad \text{par ce qui précède.} \end{aligned}$$

Lemme 2: Si $R = PQ$ dans $K[X]$, alors il existe $\tilde{P}, \tilde{Q} \in A[X]$ tq. $\tilde{R} = \tilde{P}\tilde{Q}$

Preuve 2: Écrivons $R = PQ$ avec P et $Q \in K[X]$. On prend alors $a, b \in A$ tq. $aP, bQ \in A[X]$ (par ex, a serait le produit des "dénominateurs" des coeffs de P). Alors il vient dans $A[X]$ que:

$$abR = bQ\,aP$$

En passant au contenu, le lemme précédent donne:

$$c(R) = \frac{1}{ab}\,c(aP)c(bQ)$$

Donc

$$ab = \frac{1}{c(R)}\,c(aP)c(bQ)$$

Donc,

$$R = \frac{1}{ab}\,aP\,bQ = c(R) \cdot \underbrace{\frac{aP}{c(aP)}}_{\in A[X]}\,\underbrace{\frac{bQ}{c(bQ)}}_{\in A[X]}$$

Preuve du thm : Par le lemme 2, il suffit de supposer $R = PQ$ avec $P, Q \in A[X]$ et de montrer que P ou Q est constant.

Rebelote, on projette l'égalité dans $\frac{A}{\langle p \rangle}[X]$ comme dans le thm : (avec p)

$$(*) \quad \bar{a}_m X^m = \bar{P}\bar{Q} \text{ avec } a_m \neq 0.$$

On veut utiliser l'unicité de la décomposition en facteurs irréductibles dans les anneaux factoriels. Or, p est premier, donc irréductible (on est dans un anneau factoriel), mais cela ne suffit pas à garantir que $A/\langle p \rangle$ est un corps ($\langle p \rangle$ est à priori pas maximal). Donc a priori, $\frac{A}{\langle p \rangle}[X]$ n'est à priori pas factoriel et on n'a pas l'unicité voulue.

Pour contourner le problème, on pose $L := \mathrm{Frac}\left(\frac{A}{\langle p \rangle}\right)$ et on regarde $(*)$ dans $L[X]$; par unicité de la décomposition en facteurs irréductibles dans $L[X]$,

$$\bar{Q} = \bar{b} X^r \quad \text{et} \quad \bar{P} = \bar{c} X^s$$

avec $\bar{b}\bar{c} = \bar{a}_m$ et $r+s = m$. Supposons P et Q non constants. Alors, pour des raisons de degré, $r = \deg Q$ et $s = \deg P$ (car $R = PQ$, donc $r \leq \deg Q = \deg R - \deg P \leq m - s = r$).

~~Donc bc sera le coeff dominant de $PQ = R$~~. Comme $r, s \geq 0$ par hypothèse, p divise le coeff constant de Q et de P. Donc $p^2 \mid a_0$, ce qui contredit (iii).

Remarques :

- Développement fort classique, mais somme toute agréable et sympathique ! Il paraît long ici parce que j'ai beaucoup écrit, mais on peut se contenter de rappeler des choses à l'oral, et finalement le développement se fait bien dans le temps imparti.
- On peut aussi le faire pour $A = \mathbb{Z}$ et $K = \mathbb{Q}$, et du coup, à la fin, pas besoin de prendre $\mathrm{Frac}\left(\frac{A}{\langle p \rangle}\right)$ puisque $\mathbb{Z}/p\mathbb{Z}$ est déjà un corps pour p premier.
- En petite application, il y a le fait de trouver des polynômes irréductibles sur $\mathbb{Q}$ de tout degré puisque le critère pour $p = 2$ donne $X^n - 2$ irréductible pour tout $n \geq 0$.
  Je pas trouvé d'application probante pour $A \neq \mathbb{Z}$, mais ~~sss~~ ça peut valoir le coup de chercher...