Lien entre irréductibles de $\mathbb{Q}[X]$ et de $\mathbb{Z}[X]$

On dit qu'un polynôme de $\mathbb{Z}[X]$ est **primitif** si le pgcd de ces coefficients vaut 1. On dit qu'un polynôme P est **irréductible** sur $A[X]$, s'il est non nul, non inversible dans $A[X]$ et que toute réduction $P = QR$ où $Q, R \in A[X]$ implique que soit Q, soit R est inversible. On notera $c(P)$ le **contenu** de P, autrement dit le pgcd des coefficients de P. On suppose connu le lemme de Gauss, qui dit que $c(PQ) = c(P)c(Q)$.

Théorème 1. Si $P \in \mathbb{Z}[X]$ et primitif et irréductible sur $\mathbb{Q}$, alors il est irréductible sur $\mathbb{Z}$.

Démonstration. Si P est réductible sur $\mathbb{Z}$, on peut écrire $P = QR$ où $Q, R \in \mathbb{Z}[X]$, et deg Q, deg $R \geqslant 1$ car P est primitif. Alors P est réductible sur $\mathbb{Q}$, car $Q, R \in \mathbb{Q}[X]$ et Q, R non inversible dans $\mathbb{Q}[X]$. □

Contre exemple : Si P n'est pas primitif, le résultat est faux. Par exemple $P = 2X$ est irréductible sur $\mathbb{Q}$, alors qu'il est réductible sur $\mathbb{Z}$: $P = 2 \times X$ car 2 et X ne sont pas inversibles dans $\mathbb{Z}$.

Proposition 1. Si $P \in \mathbb{Z}[X]$ est unitaire, alors P est primitif.

Démonstration. Si P est unitaire, son coefficient dominant est 1 par définition. Ainsi le pgcd de ces coefficients est 1, donc P est primitif. □

Théorème 2. Si P est irréductible sur $\mathbb{Z}$, alors soit P est une constante irréductible sur $\mathbb{Z}$, soit P est primitif de degré au moins 1 et irréductible sur $\mathbb{Q}$.

Démonstration. Soit P un polynôme irréductible sur $\mathbb{Z}$.

- Si P est un polynôme constant, alors cette constante est un irréductible de $\mathbb{Z}$ car par définition d'un irréductible, il est non nul et non inversible.
- Sinon P est un polynôme de degré au moins 1. Par contraposée, si P n'est pas primitif, *i.e.* le pgcd des coefficients (notons le d) n'est pas 1, on peut factoriser P par d et donc $P = d\tilde{P}$ où d et $\tilde{P}$ (de degré au moins 1) sont non inversibles. Donc P est réductible.

  Si P est primitif et réductible sur $\mathbb{Q}$, on peut écrire $P = QR$ où Q et R sont dans $\mathbb{Q}[X]$. On note q (resp. r) le ppcm des dénominateurs des coefficients de Q (resp. de R). On a donc qQ, $rR \in \mathbb{Z}[X]$. On peut noter $qrP = qQrR$. On a

  $$c(qrP) = qr$$

  car P est primitif. D'autre part, on a

  $$c(qQrR) = c(qQ)c(rR)$$

  car $qQ, rR \in \mathbb{Z}[X]$ et par le lemme de Gauss.

  Or $\dfrac{qQ}{c(qQ)} \in \mathbb{Z}[X]$ et $\dfrac{rR}{c(rR)} \in \mathbb{Z}[X]$, donc

  $$P = \frac{qQ}{c(qQ)} \frac{rR}{c(rR)}$$

  Donc P est réductible dans $\mathbb{Z}[X]$.

□