Polynôme minimal d'un entier d'un corps de nombres

Colas Bardavid

samedi 4 juin 2005

Table des matières

Résultats

Théorème 0.1 *Soient $P, Q \in \mathbf{Q}[X]$. Alors, $cont(PQ) = cont(P)cont(Q)$.*

Questions en suspens et travail à faire

1 Rappel sur le contenu d'un polynôme

1.1 Définition

On se place dans le cadre de $\mathbf{Z}$ mais on peut généraliser tout cela à des anneaux factoriels (c'est expliqué dans *Algebra* de Lang).

Définition 1.1 *Soit $P = \sum a_k X^k \in \mathbf{Q}[X]$ un polynôme non-nul. On appelle contenu de P et on note $cont(P)$ le nombre $\prod_{p\in\mathcal{P}} p^{\min_k v_p(a_k)}$.*

Exemple : Considérons le polynôme $P = X^3 + \frac{1}{5}X^2 + 8X + 9$. Son contenu est $\frac{1}{5}$.

1.2 Premières propriétés

Propriété 1.2 *Soit $P \in \mathbf{Q}[X]$. Alors, $P \in \mathbf{Z}[X] \iff cont(P) \in \mathbf{Z}$.*

Démonstration : Dans un sens, c'est clair.

Dans l'autre, si $cont(P) \in \mathbf{Z}$, alors, sa valuation p-adique est positive pour tout p. Donc, il en est de même pour tous les a_k et donc $P \in \mathbf{Z}[X]$. ■

Propriété 1.3 *Soit $P \in \mathbf{Q}[X]$. Notons $c = cont(P)$. Alors, $\frac{P}{c}$ est un polynôme entier de contenu 1. (On dit que P est primitif).*

Démonstration : Notons $P' = \frac{P}{c}$. Il suffit de montrer que $cont(P') = 1$. Si on note b_k le coefficient générique de P', on a $v_p(b_k) = v_p(a_k) - v_p(c)$ qui est positif ou nul tout le temps et qui vaut zéro là où le min est atteint. Ainsi, $cont(P') = 1$. ■

De façon plus générale,

Proposition 1.4 *Soit $l \in \mathbf{Q}$ et soit $P \in \mathbf{Q}[X]$. Alors, $cont(l \cdot P) = l \cdot cont(P)$.*

1.3 Multiplicativité du contenu

On démontre :

Théorème 1.5 *Soient $P, Q \in \mathbf{Q}[X]$. Alors, $cont(PQ) = cont(P)cont(Q)$.*

Démonstration : On note $x = cont(P)$ et $y = cont(Q)$. Si on réussit à démontrer que le produit de deux polynômes primitifs est primitif, on applique le résultat à $\frac{P}{x}$ et à $\frac{Q}{y}$ pour obtenir : $cont(\frac{PQ}{xy}) = 1 = \frac{cont(PQ)}{xy}$, ce qui est ce qu'on veut.

Soient donc $P, Q \in \mathbf{Z}[X]$ deux polynômes primitifs. Supposons que PQ ne soit pas primitif : soit $p \in \mathcal{P}$ tel que $p \mid cont(PQ)$, c'est-à-dire que PQ réduit modulo p est nul. C'est impossible car ni P ni Q ne sont nuls modulo p : absurde. ■

2 Polynôme minimal d'un entier algébrique

On va démontrer :

Théorème 2.1 *Soit K un corps de nombres, soit $x \in \mathcal{O}_K$. Alors, le polynôme minimal de x est à coefficients dans $\mathbf{Z}$.*

Démonstration : On sait qu'il existe $Q \in \mathbf{Z}[X]$, unitaire, tel que $Q(x) = 0$. Notons $P \in \mathbf{Q}[X]$ le polynôme minimal de x au-dessus de $\mathbf{Q}$, qu'on choisit unitaire. On sait que P divise Q dans $\mathbf{Q}[X]$: soit donc $R \in \mathbf{Q}[X]$ tel que $Q = PR$.

Notons s et t les contenus respectifs de P et R. On note $P' = \frac{P}{s}$ et $R' = \frac{R}{t}$, qui sont de contenu 1 : $P', R' \in \mathbf{Z}[X]$. On écrit : $Q = stP'R'$. On sait que $st = 1$ car Q est primitif (il vit dans $\mathbf{Z}$ et un de ses coefficients, en l'occurence le principal, vaut 1). Donc, on a $Q = P'R'$. En regardant les coefficients principaux, on voit qu'on a nécessairement (quitte à changer les signes) que P' et R' sont unitaires. Comme P l'était déjà, c'est que $s = t = 1$.

En particulier, $P \in \mathbf{Z}[X]$. ■