Université Pierre et Marie Curie 2006–2007

LM220 Maths-Info groupes 1, 2 et 5

Devoir maison n° 2

L'objectif du devoir est d'énoncer et de démontrer deux critères d'irréductibilité dans $\mathbf{Q}[X]$ pour les polynômes de $\mathbf{Z}[X]$.

1 Lemme de Gauss

Notation. Soit $P = a_0 + \cdots + a_n X^n$ un polynôme non nul de $\mathbf{Z}[X]$. On définit le *contenu* de P, noté $c(P)$, par

$$c(P) = \mathrm{pgcd}(a_0, \ldots, a_n).$$

Le polynôme P est dit *primitif* si $c(P) = 1$.

Si $P = a_0 + \cdots + a_n X^n$ et $Q = b_0 + \cdots + b_m X^m$ sont deux polynômes non nuls de $\mathbf{Z}[X]$, on se propose de montrer que

$$c(PQ) = c(P)c(Q). \qquad (\star)$$

1.1 Posons $PQ = \sum_{k \geqslant 0} c_k X^k$. Exprimer chaque c_k en fonction des coefficients (a_i) et (b_j) de P et Q.

1.2 On suppose, *dans cette question*, les polynômes P et Q primitifs : $c(P) = c(Q) = 1$. On souhaite montrer que $c(PQ) = 1$. On raisonne par l'absurde en supposant qu'il existe un nombre premier p divisant $c(PQ)$.

1.2.1 Montrer qu'il existe i_0 et j_0 deux entiers $\geqslant 0$ tels que

$$\begin{array}{ll} \text{pour tout } i < i_0, \text{ on a } p \mid a_i, & \text{mais } p \nmid a_{i_0}, \\ \text{pour tout } j < j_0, \text{ on a } p \mid b_j, & \text{mais } p \nmid b_{j_0}. \end{array}$$

1.2.2 En remarquant que p divise $c_{i_0+j_0}$, déduire une contradiction (*Indication* : on montre que p divise $a_{i_0} b_{j_0}$.).

1.2.3 En déduire que, si P et Q sont primitifs, alors $c(PQ) = 1 = c(P)c(Q)$.

1.3 Montrer qu'il existe $\widetilde{P}$ et $\widetilde{Q}$ deux polynômes primitifs tels que

$$P = c(P)\widetilde{P} \quad \text{et} \quad Q = c(Q)\widetilde{Q}.$$

1.4 En déduire la relation $(\star)$ (lemme de Gauss).

2 Irréductibilité dans $\mathbf{Z}[X]$ et $\mathbf{Q}[X]$

Soit P un polynôme de $\mathbf{Z}[X]$. On se propose de démontrer que P est le produit de deux polynômes non constants de $\mathbf{Z}[X]$ si et seulement si P est le produit de deux polynômes non constants de $\mathbf{Q}[X]$.

On suppose pour cela que

$$P = QR \quad \text{avec } Q \text{ et } R \text{ deux polynômes de } \mathbf{Q}[X] \text{ non constants.}$$

2.1 Soit m le ppcm des dénominateurs des coefficients de Q écrits sous forme de fractions irréductibles.

2.1.1 Montrer que $mQ \in \mathbf{Z}[X]$.

2.1.2 Dites pourquoi le polynôme

$$\widetilde{Q} = \frac{m}{c(mQ)} Q$$

est un polynôme primitif de $\mathbf{Z}[X]$.

2.1.3 Montrer que m et $c(mQ)$ sont premiers entre eux.

2.2 On écrit de même

$$R = \frac{c(m'R)}{m'} \widetilde{R}, \quad \text{avec } \widetilde{R} \text{ primitif.}$$

Les entiers m' et $c(m'R)$ sont premiers entre eux. Démontrer la relation suivante

$$mm'c(P) = c(mQ)c(m'R).$$

2.3 En déduire que $\frac{mQ}{m'}$ et $\frac{m'R}{m}$ sont dans $\mathbf{Z}[X]$.

2.4 Conclure à l'équivalence annoncée.

Dans les parties 3 et 4, $P = a_0 + \cdots + a_n X^n$ désigne un polynôme non constant de $\mathbf{Z}[X]$ et p un nombre premier. Si $a \in \mathbf{Z}$, on note $\overline{a}$ sa réduction modulo p. De même, si $A \in \mathbf{Z}[X]$, on note $\overline{A}$ le polynôme de $\mathbf{F}_p[X]$ déduit de A par réduction modulo p de ses coefficients.

3 Critère d'Eisenstein

On suppose ici que les trois conditions suivantes sont satisfaites :

1. on a $p \nmid a_n$,
2. pour tout $0 \leqslant i \leqslant n-1$, on a $p | a_i$,

3. on a $p^2 \nmid a_0$.

On va montrer que, sous ces hypothèses, le polynôme P est irréductible dans $\mathbf{Q}[X]$. On raisonne par l'absurde en supposant que

$$P = QR \quad \text{avec } Q \text{ et } R \text{ deux polynômes de } \mathbf{Q}[X] \text{ non constants.}$$

3.1 Dites pourquoi on peut supposer Q et R à coefficients entiers.

3.2 On suppose désormais que tel est le cas et on écrit

$$\begin{aligned} Q &= b_0 + \cdots + b_q X^q, \qquad \text{avec } b_i \in \mathbf{Z}, \\ R &= c_0 + \cdots + c_r X^r, \qquad \text{avec } c_i \in \mathbf{Z}. \end{aligned}$$

Montrer que, dans $\mathbf{F}_p[X]$, on a l'égalité

$$\overline{a_n} X^n = (\overline{b_0} + \cdots + \overline{b_q} X^q)(\overline{c_0} + \cdots + \overline{c_r} X^r).$$

3.3 En déduire que $\overline{b_i} = \overline{0}$ pour $i < q$ et $\overline{c_j} = \overline{0}$ pour $j < r$.

3.4 Conclure à une contradiction.

3.5 Montrer, avec le critère précédent, que le polynôme $P = 3X^4 + 15X^2 + 10$ est irréductible dans $\mathbf{Q}[X]$.

4 Réduction modulo p

On suppose dans cette partie que p ne divise pas a_n et que le polynôme

$$\overline{P} = \overline{a_0} + \cdots + \overline{a_n} X^n$$

est irréductible dans $\mathbf{F}_p[X]$.

On va montrer que sous ces hypothèses, le polynôme P est irréductible dans $\mathbf{Q}[X]$. On raisonne encore par l'absurde. On écrit alors, comme à la question 3.1 :

$$P = QR \quad \text{avec } Q \text{ et } R \text{ deux polynômes non constants de } \mathbf{Z}[X].$$

4.1 Montrer que $\deg(\overline{Q}) = \deg(Q)$ et $\deg(\overline{R}) = \deg(R)$.

4.2 En déduire que $\deg(\overline{Q}) = 0$ ou $\deg(\overline{R}) = 0$ et conclure à l'irréductibilité de P dans $\mathbf{Q}[X]$.

4.3 Application. Montrer que le polynôme

$$P = X^3 + 462X^2 + 2433X - 67691$$

est irréductible dans $\mathbf{Q}[X]$.

Remarque. La condition ci-dessus est suffisante mais n'est pas nécessaire. On a vu en exercice que le polynôme $P = X^4 + 1$ est irréductible dans $\mathbf{Q}[X]$, mais on peut montrer qu'il est réductible dans $\mathbf{F}_p[X]$ pour tout nombre premier p.