Polynômes irréductibles sur $\mathbb{Z}$, réductibles sur $\mathbb{F}_p$ pour tout p

Benjamin Hellouin

Francinou-Gianella alg.1 (le vieux)

Lemme 1. *Soit K un corps, $P \in K[X]$ de degré n. Montrer que P est irréductible si et seulement s'il n'admet aucune racine dans les extensions L de K telles que $[L : K] \leq n/2$.*

Preuve du lemme. Supposons P irréductible, et soit L une décomposition dans laquelle P admet une racine. Alors $K \subset K(x) \subset L$, et en particulier $[L : K] \geq n$.

Inversement, supposons que $P = P_0 P_1$ dans $K[X]$. Alors un des deux polynômes est de degré $\leq n/2$, ce qui implique que P possède un facteur irréductible Q de degré $\leq n/2$. Soit L un corps de rupture de Q sur K : on a $[L : K] = \deg Q \leq n/2$ et P admet une racine sur L.

Théorème 1. *On pose $P(X) = X^4 + 1$. Alors P est irréductible sur $\mathbb{Z}$, mais sa réduction mod p est réductible sur $\mathbb{F}_p$, et ce pour tout p.*

Preuve. Pour prouver que P est irréductible sur $\mathbb{Z}$, on considère $P(X+1) = X^4 + 4X^3 + 6X^2 + 4X + 1$. Clairement, $P(X+1)$ est réductible si et seulement si $P(X)$ est réductible. Or, le critère d'Eisenstein pour $p = 2$ garantit que ce second polynôme est irréductible sur *mathbbZ*.

Traitons le cas $p = 2$: on a $X^4 + 1 = (X + 1)^4$ (morphisme de Frobénius).

Soit enfin p premier impair. On peut écrire dans $\mathbb{F}_p[X]$

$$(X^8 - 1) = (X^4 - 1)(X^4 + 1).$$

En particulier, si x est une racine de $X^4 + 1$ dans une extension K de $\mathbb{F}_p$, on a $x^8 = 1$ et $x^4 \neq 1$ (car $1 \neq -1$ pour $p > 2$). Donc trouver une racine de $(X^4 + 1)$ revient à trouver un élément d'ordre 8 dans K^*.

Considérons en particulier $K = \mathbb{F}_{p^2}$. $\mathbb{F}_{p^2}^*$ est un groupe cyclique (comme tout groupe multiplicatif d'un corps) et il est d'ordre $p^2 - 1 = (p-1)(p+1)$. $(p-1)$ et $(p+1)$ sont deux nombres pairs consécutifs, donc l'un deux est divisible par 4 et leur produit est divisible par 8. Donc il existe un (unique) sous-groupe cyclique d'ordre 8 dans $F_{p^2}^*$, et il suffit de prendre un générateur pour obtenir une racine de $X^4 + 1$.

P admet donc une racine dans $\mathbb{F}_{p^2}$ qui est une extension de degré $2 \leq \deg P/2$, et par le lemme préliminaire, on en déduit que P est réductible dans $\mathbb{F}_p$.