

Nombre de polynômes irréductibles de degré n sur un corps fini (Ortisz + Itard page 66-67)

Pierre Lissy

May 19, 2010

Lemme 1. *On a le fait suivant: Q irréductible de degré d divise $X^{p^n} - X$ ssi $d|n$.*

Proof. Q est irréductible de degré d . Donc $F_p/(Q)$ est un corps K qui est en fait F_{p^d} . Notamment, le groupe des inversibles du corps est cyclique et il existe un élément d'ordre $p^d - 1$, noté y . y vérifie $y^{p^d} = y$. De plus, $y = R(\bar{X})$ avec R de degré inférieur à $d - 1$. Enfin l'ordre de $\bar{X}$ divise $p^d - 1$. Remarquons que $p^d - 1$ divise $p^n - 1$ ssi $d|n$. En effet, si on écrit $n = dq + r$, on a $p^n - 1 = p^{dq+r} - 1 = p^r(p^{dq} - 1) + p^r - 1$ et donc le reste de la division est $p^r - 1$, nul si et seulement si $r = 0$. On peut alors conclure. Si $d|n$ alors l'ordre de $\bar{X}$ divise $p^n - 1$ ce qui signifie exactement que $Q|X^{p^n} - X$. Inversément, si $Q|X^{p^n} - X$, alors comme $X^{p^n} = X$ on obtient par Frobenius que $R(\bar{X})^{p^n} = R(\bar{X})$, donc $y^{p^n} = y$ et on a bien que $p^d - 1|p^n - 1$ ce qui implique $d|n$. $\square$

Corollaire 1. $X^{p^n} - X = \prod_{d|n} \prod_{Q \in K_p^d} Q$.

Proof. En effet, d'abord clairement $X^{p^n} - 1$ est sans facteur carré puisque son corps de décomposition est F^{p^n} tout entier. Mais on sait en outre grâce à ce qui précède et en utilisant le fait que deux polynômes irréductibles non associés sont premiers entre eux que $\prod_{d|n} \prod_{Q \in K_p^d} Q | X^{p^n} - X$. Mais inversément le point précédent nous assure que si on décompose notre polynôme en irréductibles, les facteurs irréductibles qui apparaissent ne peuvent être autre chose que les éléments des K_p^d . D'où l'égalité car les polynômes sont unitaires. $\square$

Corollaire 2. $p^n = \sum_{d|n} dI_d^p$

Proof. Il suffit de prendre les degrés dans l'égalité précédente. $\square$

Théorème 1. $I_n^d = 1/n \sum_{d|n} \mu(n/d) q^d$

Proof. C'est immédiat par la relation d'inversion de Moebius. Rappelons que si f est une fonction de $\mathbb{R}^+$ à valeurs réelles nulle pour $x < 1$, et si on pose $F(x) = \sum_{n=0}^{\infty} f(x/n)$, alors on peut former un tableau suivant:

$$\begin{aligned} F(x)\mu(1) &= f(x) + f(x/2) + \dots \\ F(x/2)\mu(2) &= -f(x/2) - f(x/4) - \dots \\ F(x/3)\mu(3) &= -f(x/6) - f(x/9) - \dots \\ F(x/4) &= 0 * F(x/4) + \dots \end{aligned}$$

et ainsi de suite. On voit qu'en sommant par colonnes, on obtient $f(x) = \sum_1^{\infty} \mu(n)F(x/n)$. Ici, on a $f(x) = xI_x^p$ pour x entier, 0 sinon. Du coup, on a $F(x) = \sum_{x|n} dI_x^p$ pour x entier (et ceci vaut d'après ce qui précède q^x , 0 sinon). Par inversion, $f(x) = \sum_1^{\infty} \mu(n)F(x/n) = \sum_{d|n} \mu(d)q^{d/n} = \sum_{d|n} \mu(n/d)q^d$ (car l'application $d \mapsto n/d$ est une bijection des diviseurs de n sur lui-même). $\square$

References

[1]