Développement d'algèbre : Nombre de polynômes irréductibles sur $\mathbb{F}_p$

2021

1 Introduction

L'objectif est de démontrer l'existence de corps de cardinal $q = p^n$ où p est premier, en tant que corps de rupture sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ d'un polynôme irréductible unitaire de degré n. Nous devons garantir que de tels polynômes existent. Pour ce faire, on va les compter et voir qu'il en existe au moins un. Ce développement est relativement facile mais il est tout à fait possible de le présenter à l'oral sans en rougir, d'autant qu'il utilise beaucoup de propriétés élémentaires sur les corps finis. Il est tiré du Rombaldi, *Mathématiques pour l'agrégation, Algèbre et géométrie.*

2 Le développement

Soit p un nombre premier.

Théorème 1. *Pour $n \in \mathbb{N}^*$, il existe un polynome irréductible unitaire de degré n sur $\mathbb{F}_p$.*

Observons que le corollaire annoncé de ce théorème est l'existence d'un corps de cardinal p^n. Pour démontrer ce théorème, on introduit le polynôme $P_n = X^{p^n} - X \in \mathbb{F}_p[X]$ de degré p^n. On note I_d l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_p$ de degré d. On va montrer les trois lemmes suivants :

Lemme 1. *Soit $P \in \mathbb{F}_p$ un polynôme irréductible unitaire de degré d. Alors d divise n si et seulement si P divise P_n*

Lemme 2. *Le polynôme P_n se factorise en $P_n = \prod_{d|n} \left(\prod_{P \in I_d} P \right)$.*

Lemme 3. *Si μ représente la fonction de Möbius, on a*

$$n|I_n| = \sum_{d|n} \mu(\frac{n}{d}) p^d.$$

Preuve du lemme 1. On note K le corps $K = \mathbb{F}_p[X]/(P)$, ce qui est possible car P est irréductible sur $\mathbb{F}_p$. On notera désormais $\overline{Q}$ l'image par le morphisme de quotient d'un polynôme $Q \in \mathbb{F}_p[X]$. Supposons $d|n$. Le groupe K^* possède $p^d - 1$ éléments, donc par théorème de Lagrange, tous ses éléments vérifient $\overline{Q}^{p^d-1} = 1$. En particulier, $\overline{X}^{p^d-1} = 1$, d'où $\overline{X}^{p^d} = \overline{X}$. Par récurrence sur $k \in \mathbb{N}$ on obtient donc $\overline{X}^{p^{kd}} = \overline{X}$. Comme n est un multiple de d, on a finalement $\overline{X}^{p^n} = \overline{X}$ donc $\overline{P_n} = 0$ et donc $P_n \in (P)$.

Réciproquement, supposons $P|P_n$. On a alors $\overline{P_n} = 0$, c'est-à-dire $\overline{X}^{p^n} = \overline{X}$. On va voir que les éléments $\overline{Q} = \sum_{k=0}^{d-1} a_k \overline{X}^k \in K^*$ vérifient $\overline{Q}^{p^n} = \overline{Q}$. En effet, comme K est de caractéristique p (son sous corps premier ne saurait être autre que $\mathbb{F}_p$), par propriété de Frobénius on a

$$\overline{Q}^{p^n} = \left(\sum_{k=0}^{d-1} a_k \overline{X}^k \right)^{p^n} = \sum_{k=0}^{d-1} a_k^{p^n} \overline{X}^{kp^n} = \sum_{k=0}^{d-1} a_k^{p^n} \overline{X}^k.$$

Or par le petit théorème de fermat, on a $a_k^p = a_k$ donc $a_k^{p^n} = a_k$. Donc on a $\overline{Q}^{p^n} = \overline{Q}$, soit encore $\overline{Q}^{p^n-1} = 1$. Ceci est vrai pour tous les éléments de K^*, et en particulier, comme K^* est cyclique, c'est vrai pour un générateur $\overline{Q_0}$ de K^*. ce dernier étant d'ordre $|K^*| = p^d - 1$, on conclut donc que $p^d - 1 = \omega(\overline{Q_0})$ divise $p^n - 1$. Si on écrit $n = ds + r$ avec $0 \leqslant r < d - 1$, on a donc pour un certain $a \in \mathbb{N}$ et $b = \sum (p^d)^k$:

$$a(p^d - 1) = p^n - 1 = (p^d)^s p^r - 1 = ((p^d)^s - 1)p^r + p^r - 1 = (p^d - 1)bp^r + p^r - 1$$

donc $(p^d - 1)(a - bp^r) = p^r - 1$ et $p^d - 1$ divise $p^r - 1$. Supposer $r \neq 0$ est alors absurde car $r < d$. Donc $r = 0$ et d divise n. □

Preuve du lemme 2. Il suffit de montrer que P_n n'a pas de facteur carré. En effet la factorisation annoncée est alors exactement la décomposition de P_n en facteurs irréductibles d'après le lemme 1. Le polynôme $P_n' = p^n X^{p^n-1} - 1 = -1$ étant constant dans $\mathbb{F}_p$, le polynôme P_n n'a pas de facteur carré dans $\mathbb{F}_p$. □

Preuve du lemme 3. On considère le degré de P_n. D'une part comme $P_n = X^{p^n} - X$, on a $\deg(P_n) = p^n$, et d'autre part l'expression de P_n fournie par le lemme 2 donne

$$p^n = \deg(P_n) = \sum_{d|n} \sum_{P \in I_d} \deg(P) = \sum_{d|n} d|I_d|.$$

D'après la formule d'inversion de Möbius, on obtient le résultat souhaité. □

Preuve du théorème. Il s'agit de montrer que $|I_n| > 0$. On a d'après le lemme 3 :

$$n|I_n| = p^n + \sum_{d|n, d \neq n} p^d \mu\left(\frac{n}{d}\right).$$

Les diviseurs propres de n sont tous plus petits que $\frac{n}{2}$. D'autre part, il y a au plus $\frac{n}{2}$ termes non nuls dans la somme, d'où

$$\left| \sum_{d|n, d \neq n} p^d \mu\left(\frac{n}{d}\right) \right| \leqslant \frac{n}{2} p^{n/2}.$$

Comme $\frac{p^n}{\frac{n}{2}p^{n/2}} = \frac{2}{n}p^{n/2}$, et $x \mapsto \frac{p^x}{x}$ est croissante et vaut $p \geqslant 2$ en 1, p^n est strictement supérieur à la somme de tous les autres termes. Finalement, on a bien $n|I_n| > 0$. On obtient même facilement l'équivalent $I_n \sim \frac{p^n}{n}$. □