
Corps finis – Exercices théoriques

Exercice 1. Soit p premier et $n \geq 2$ entier. On note k le corps à p éléments et K un corps à p^n éléments. On note F le morphisme de Frobenius de K .

1. Montrer que $F^n = \text{Id}$.
2. Soit $\hat{F} : K[X] \rightarrow K[X]$ l'application définie par $\hat{F}(\sum_{i=0}^m a_i X^i) = \sum_{i=0}^m F(a_i) X^i$. Montrer que \hat{F} est un morphisme d'anneaux et que pour $P \in K[X]$, $\hat{F}(P) = P$ si et seulement si P est à coefficients dans k .
3. Soit $P \in k[X]$ et $\alpha \in K$ tel que $P(\alpha) = 0$.
 - (a) Montrer que $F(\alpha)$ est également une racine de P sur K .
On note ℓ le plus petit entier $j \geq 1$ tel que $\alpha^{p^j} = \alpha$.
 - (b) Justifier l'existence de ℓ et montrer que $\ell \leq n$.
 - (c) Montrer que $\alpha, \alpha^p, \dots, \alpha^{p^{\ell-1}}$ sont deux à deux distincts.
 - (d) Montrer que $Q = \prod_{i=0}^{\ell-1} (X - \alpha^{p^i})$ est à coefficients dans k .
 - (e) Montrer qu'il existe $R \in k[X]$ tel que $P = QR$.

Exercice 2. Soit p un nombre premier supérieur à 6. On considère les nombres de Fibonacci dans \mathbb{F}_p , c'est à dire les éléments de \mathbb{F}_p définis par

$$F_0 = 0, F_1 = 1 \quad \text{et} \quad \forall n \geq 0, F_{n+2} = F_{n+1} + F_n.$$

On pose $P = X^2 - X - 1 \in \mathbb{F}_p[X]$.

1. Montrer que P est irréductible sur \mathbb{F}_p si et seulement si il existe $a \in \mathbb{F}_p$ tel que $(2a - 1)^2 = 5$. Dans ce cas, donner les racines de P .
2. On suppose qu'il existe $a \in \mathbb{F}_p$ tel que $(2a - 1)^2 = 5$. Donner une formule explicite pour les nombres de Fibonacci dans \mathbb{F}_p en fonction de a .