Les polynômes irréductibles sur $K[X]$

PAR SABIR ILYASS

L'OBJECTIF:

Soit K un corps commutatif fini, on veut trouver le nombre des polynômes irréductibles sur $K[X]$ de degré n.

⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆

Théorème 1.

Il existe un nombre premier p et un entier $n \in \mathbb{N}$, tel que $\# K = p^n$

Démonstration. □

Notons L le plus petit sous corps de K.

Puisque K est fini, alors il existe un nnombre premier p tel que L est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, en particulier $\# L = p$.

On note : $n = [K : \mathbb{Z}/\mathrm{pZ}] = \dim_L(K) < +\infty$

On a K est un L espace-vectoriel de dimension n. notons $\mathcal{B} = (e_1, \ldots, e_n)$ une base de K comme L espace-vectoriel, de plus l'application : $\begin{array}{ccc} L^n & \rightarrow K \\ (x_1, \ldots, x_n) & \longmapsto \sum_{k=1}^{n} x_k e_k \end{array}$ est bijective, en particulier :

$$\boxed{\# K = \#(L^n) = p^n}$$

⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆

On note pour tout entier $n \in \mathbb{N}^\star$, $\mathcal{P}_K(n)$ l'ensemble des polynômes unitaires, irréductibles de degré n sur $K[X]$.

On a bien pour tout polynôme $P \in K[X]$ irréductible, pour tout $a \in K \setminus \{0\}$ $a.P$ est irréductible sur $K[X]$.

En a alors pour tout entier $n \in \mathbb{N}^\star$, le nombre des polynômes irréductibles de degré n est :

$$(\# K - 1).\# \mathcal{P}_K(n)$$

Il ne reste qu'a trouver le cardinal de $\mathcal{P}_K(n)$, pour tout $n \in \mathbb{N}^\star$.

Théorème 2.

Notons $\#K = q$, Soit $n \in \mathbb{N}^\star$, on a

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_K(d)} P(X)$$

Démonstration. $\square$

Pour tout entier $d \in \mathbb{N}^\star$, et pour tout $P \in \mathcal{P}_K(d)$, on a $M = K/(P)$ est un corps (car K est principal), de cardinal q^d , donc isomorphe à $\mathbb{Z}/q^d\mathbb{Z}$:

$$\forall x \in M, x^{q^d} = x$$

Mais si $n = d.k$ pour un $k \in \mathbb{N}^\star$, on a

$$x^{q^n} = x^{q^{d.k}} = (((x^{q^d})^{q^d})\ldots)^{q^d} \quad (k\,\text{fois})$$

par une récurrence immédiate sur k, ceci est égal à x. Autrement dit,

$$X^{q^n} - X = 0 \in M[X]$$

donc P divise $X^{q^n} - X$ dans $K[X]$.

Comme les éléments de $\mathcal{P}_K(d)$ sont irréductibles, le produit $\prod_{d|n} \prod_{P \in \mathcal{P}_K(d)} P(X)$ divise lui aussi $X^{q^n} - X$.

Réciproquement, soit P un facteur irréductible de degré d de $X^{q^n} - X$ dans $K[X]$, comme $\mathbb{Z}/q^n\mathbb{Z}$ est un corps de décomposition de $X^{q^n} - X$, P est scindé sur $\mathbb{Z}/q^n\mathbb{Z}$.

Si x est une racine de P, on a

$$[\mathbb{Z}/q^n\mathbb{Z} : \mathbb{Z}/q\mathbb{Z}] = n = [\mathbb{Z}/q^n\mathbb{Z} : \mathbb{Z}/q\mathbb{Z}(x)][\mathbb{Z}/q\mathbb{Z}(x) : \mathbb{Z}/q\mathbb{Z}]$$

Mais comme P est irréductible, $\mathbb{Z}/q\mathbb{Z}(x)$ est un corps de rupture de P de degré d sur $\mathbb{Z}/q\mathbb{Z}$, donc d divise n. Il suffit alors de montrer que $X^{q^n} - X$ n'admet pas de facteur double (ou plus) : si il existe un tel facteur, alors $X^{q^n} - X$ admet une racine double dans un corps de décomposition. Cependant, comme le polynôme dérivé de $X^{q^n} - X$ est $q^n X^{q^n - 1} - 1 = -1$ (à cause de la caractéristique),

$X^{q^n} - X$ n'a pas de racine double dans un corps de décomposition, ce qui termine la preuve.

Définition 1.(la fonction de Möbius)

Soit $n \in \mathbb{N}^\star$, On note $\mu(n)$ l'entier défini par :

$$\mu(n)=\begin{cases} 0 \quad \text{si } n \text{ est divisible par le carré } d\text{'un nombre premier} \\ (-1)^r \quad \text{si } r \text{ est le nombre de facteurs premiers distincts de } n\,, \\ n \text{ non divisible par le carré } d\text{'un nombre premier} \end{cases}$$

Proposition 1.

pour tout $n \neq 1$, on a l'égalité

$$\sum_{d|n} \mu(d) = 0$$

Démonstration. (Proposition 1) □

Méthode 1 : soit $n = \prod_{i=1}^{m} p_i^{a_i}$ la décomposition en facteurs premiers de n,

De plus si $d \in \mathbb{N}$, alors :

d/n et $\mu(d) \neq 0$ si et seulement si $d = \prod_{i \in J} p_i^{a_i}$ with $J \subset [\![1, m]\!]$ et alors $\mu(d) = (-1)^{\#J}$, on en déduit que

$$\boxed{\sum_{d|n} \mu(d) = \sum_{J \subset [\![1,m]\!]} (-1)^{\#J} = (1-1)^m = 0} \text{(car } m > 0)$$

Méthode 2 :Soit $n \geqslant 2$, d'après le théorème fondamentale de l'arithmétique on a l'existance de $(p_1, \ldots, p_r) \in \mathcal{P}^r$ et $\alpha_1, \ldots, \alpha_r \geqslant 1$ tel que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$

On a

$$\sum_{d|n} \mu(d) = \sum_{k_1=0}^{\alpha_1} \sum_{k_2=0}^{\alpha_2} \cdots \sum_{k_r=0}^{\alpha_r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Parsuite:

$$\sum_{d|n} \mu(d) = \sum_{\substack{(k_1,\ldots,k_r) \in \prod_{i=1}^{r} [\![0,\alpha_i]\!] \\ \exists i_0 \in [\![1,r]\!]\, k_{i_0} \geqslant 2}} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) + \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

puisque pour tout $(k_1, \ldots, k_r) \in \prod_{i=1}^{r} [\![0, \alpha_i]\!]$ tel que $\exists i_0 \in [\![1, r]\!]\, k_{i_0} \geqslant 2$

On a $\prod_{i=1}^{r} p_i^{k_i}$ est divisible par $p_{i_0}^2$ alors $\mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)=0$

D'où

$$\sum_{\substack{(k_1,\ldots,k_r)\in \prod_{i=1}^{r} [\![0,\alpha_i]\!] \\ \exists i_0\in[\![1,r]\!]\, k_{i_0}\geqslant 2}} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)=0$$

Par suite

$$\sum_{d|n}\mu(d)=\sum_{(k_1,\ldots,k_r)\in[\![0,1]\!]^r}\mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Pour tout $(k_1,\ldots,k_r)\in[\![0,1]\!]^r$,on a $\sum_{i=1}^{r} k_i$ est le nombre de facteurs premiers distincts de $\prod_{i=1}^{r} p_i^{k_i}$, et $\prod_{i=1}^{r} p_i^{k_i}$ est non divisible par le carré d'un nombre premier, alors

$$\boxed{\sum_{d|n}\mu(d)=\sum_{(k_1,\ldots,k_r)\in[\![0,1]\!]^r}(-1)^{\sum_{i=1}^{r} k_i}=\prod_{i=1}^{r}\left(\sum_{k_1=0}^{1}(-1)^{k_i}\right)=(1-1)^r=0}$$

Théorème 3.(la formule d'inversion de Möbius)

Soit H une fonction non nulle de $\mathbb{N}^\star$ dans $\mathbb{C}$ telle que $\forall n,m\in N, H(n.m)=H(n)H(m)$

Et on se donne également deux fonctions F et G de $[1,+\infty[$ dans $\mathbb{C}$ telles que :

$$\forall x>1, G(x)=\sum_{1\leqslant k\leqslant x} F\left(\frac{x}{k}\right)H(k)$$

Alors:

$$\forall x>1, F(x)=\sum_{1\leqslant k\leqslant x} \mu(k)G\left(\frac{x}{k}\right)H(k)$$

Démonstration. □

on a $H(1)=H(1\times 1)=H(1)^2$, et puisque $H\neq 0$ alors $H(1)=1$
et on a pour tout $x\in[1,+\infty[$

$$\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)H(k)=\sum_{1\leqslant k\leqslant x}\mu(k)\sum_{1\leqslant i\leqslant \frac{x}{k}} F\left(\frac{x}{i.k}\right)H(i)H(k)$$

Par suite

$$\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)H(k)=\sum_{1\leqslant k\leqslant x}\sum_{1\leqslant i\leqslant \frac{x}{k}}\mu(k)F\left(\frac{x}{i.k}\right)H(i.k)$$

Ainsi

$$\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)H(k)=\sum_{1\leqslant k.i\leqslant x}\mu(k)F\left(\frac{x}{i.k}\right)H(i.k)$$

Ainsi

$$\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)H(k)=\sum_{1\leqslant m\leqslant x}\sum_{d|m}\mu(d)F\left(\frac{x}{m}\right)H(m)$$

Par suite

$$\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)H(k)=\sum_{1\leqslant m\leqslant x}F\left(\frac{x}{m}\right)H(m)\left(\sum_{d/m}\mu(d)\right)$$

Ainsi

$$\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)H(k)=F(x)H(1)+\sum_{2\leqslant m\leqslant x}F\left(\frac{x}{m}\right)H(m)\left(\sum_{d/m}\mu(d)\right)$$

D'après la proposition 1, on a pour tout $m\geqslant 2$

$$\sum_{d|m}\mu(d)=0$$

d'où

$$\boxed{F(x)=\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)H(k)}$$

Corollaire 1.
On a pour tout entier $n\in\mathbb{N}^\star$

$$\#\mathcal{P}_K(n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)(\#K)^d$$

Démonstration. $\square$

Soit $n\in\mathbb{N}^\star$, notons $\#K=q$, on a d'après théorème 1

$$X^{q^n}-X=\prod_{d|n}\prod_{P\in\mathcal{P}_K(d)}P(X)$$

Donc

$$q^n=\deg(X^{q^n}-X)=\sum_{d|n}\sum_{P\in\mathcal{P}_K(d)}\deg(P(X))=\deg\left(\prod_{d|n}\prod_{P\in\mathcal{P}_K(d)}P(X)\right)$$

Par suite

$$\sum_{d|n}d.\#\mathcal{P}_K(d)=q^n$$

D'où d'après la formule d'inversion de Möbius

$$\boxed{\#\mathcal{P}_K(n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)(\#K)^d}$$

⋆⋆⋆⋆⋆⋆⋆⋆⋆⋆

Pour aller plus loin:

On veut trouver le nombre des polynômes irréductibles sur $K[X]$.

On a le nombre des polynômes irréductibles sur $K[X]$ est :

$$\sum_{n=1}^{+\infty}(\#K-1).\#\mathcal{P}_K(n)=(\#K-1)\sum_{n=1}^{+\infty}\#\mathcal{P}_K(n)$$

Donc, le nombre des polynômes irréductibles sur $K[X]$ est :

$$(\#K-1)\sum_{n=1}^{+\infty}\#\mathcal{P}_K(n)=(\#K-1)\sum_{n=1}^{+\infty}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)(\#K)^d$$

Pour simplifier l'écriture, on pose $\#K=q$,et on a

$$\sum_{n=1}^{+\infty}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d=\sum_{n=1}^{+\infty}\sum_{d|n}\frac{1}{n}\mu\left(\frac{n}{d}\right)q^d$$

Donc

$$\sum_{n=1}^{+\infty}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d=\sum_{n=1}^{+\infty}\sum_{d=1}^{+\infty}\frac{1}{n}\mu\left(\frac{n}{d}\right)1_{\mathbb{N}}\left(\frac{n}{d}\right)q^d$$

Avec $\mu(r)=0$, pour les nombres rationnels (on définit tout simplement un prolongement de μ qui n'a pas d'influence sur le résultat de la somme ,puisque $1_{\mathbb{N}}(r)=0$ si r n'est pas entier)

On a alors d'après le théorème de Fubini et par positivité des termes de la somme

$$\sum_{n=1}^{+\infty}\frac{1}{n}\sum_{d\mid n}\mu\left(\frac{n}{d}\right)q^d=\sum_{d=1}^{+\infty}\sum_{n=1}^{+\infty}\frac{1}{n}\mu\left(\frac{n}{d}\right)1_{\mathbb{N}}\left(\frac{n}{d}\right)q^d$$

Ainsi

$$\sum_{n=1}^{+\infty}\frac{1}{n}\sum_{d\mid n}\mu\left(\frac{n}{d}\right)q^d=\sum_{d=1}^{+\infty}\sum_{n=1}^{+\infty}\frac{1}{d.n}\mu(n)q^{d.n}$$

Par suite:

$$\sum_{n=1}^{+\infty}\frac{1}{n}\sum_{d\mid n}\mu\left(\frac{n}{d}\right)q^d=\sum_{d=1}^{+\infty}\frac{1}{d}\sum_{n=1}^{+\infty}\frac{1}{n}\mu(n)(q^d)^n$$

Pour tout entier $d\in\mathbb{N}^\star$, essayons de calculer la somme de la série $\sum_{n\geqslant 1}\frac{1}{n}\mu(n)(q^d)^n$

Notons pour tout $r\in\mathbb{N}^\star$, p_r le r-ième nombre premier.

On a pour tout $N\in\mathbb{N}^\star$, par définition de la fonction de Möbius:

$$\sum_{n_1=0}^{+\infty}\sum_{n_2=0}^{+\infty}\cdots\sum_{n_N=0}^{+\infty}\frac{1}{\prod_{i=1}^{N}p_i^{n_i}}\mu\left(\prod_{i=1}^{N}p_i^{n_i}\right)(q^d)^{\prod_{i=1}^{N}p_i^{n_i}}=\sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N}p_i^{n_i}}\mu\left(\prod_{i=1}^{N}p_i^{n_i}\right)(q^d)^{\prod_{i=1}^{N}p_i^{n_i}}$$

Avec:

$$\sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N}p_i^{n_i}}\mu\left(\prod_{i=1}^{N}p_i^{n_i}\right)(q^d)^{\prod_{i=1}^{N}p_i^{n_i}}=\sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N}p_i^{n_i}}(-1)^{\sum_{i=1}^{N}n_i}(q^d)^{\prod_{i=1}^{N}p_i^{n_i}}$$

Ainsi

$$\sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N}p_i^{n_i}}\mu\left(\prod_{i=1}^{N}p_i^{n_i}\right)(q^d)^{\prod_{i=1}^{N}p_i^{n_i}}=\sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N}(-p_i)^{n_i}}(q^d)^{\prod_{i=1}^{N}p_i^{n_i}}$$

Calculons maintenant $\sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N}(-p_i)^{n_i}}(q^d)^{\prod_{i=1}^{N}p_i^{n_i}}$

Notons $A_N=\sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N}(-p_i)^{n_i}}(q^d)^{\prod_{i=1}^{N}p_i^{n_i}}$,pour tout entier $N\in\mathbb{N}^\star$

On a

$$\sum_{n_N=0}^{1}\frac{1}{\prod\limits_{i=1}^{N}(-p_i)^{n_i}}(q^d)^{\prod\limits_{i=1}^{N}p_i^{n_i}}=\frac{1}{\prod\limits_{i=1}^{N-1}(-p_i)^{n_i}}\sum_{n_N=0}^{1}\frac{1}{(-p_N)^{n_N}}\left((q^d)^{\prod\limits_{i=1}^{N-1}p_i^{n_i}}\right)^{n_N}$$

Par suite

$$\sum_{n_N=0}^{1}\frac{1}{\prod\limits_{i=1}^{N}(-p_i)^{n_i}}(q^d)^{\prod\limits_{i=1}^{N}p_i^{n_i}}=\frac{1}{\prod\limits_{i=1}^{N-1}(-p_i)^{n_i}}\left(1-\frac{1}{p_N}(q^d)^{\prod\limits_{i=1}^{N-1}p_i^{n_i}}\right)$$

Ainsi

$$A_N=\sum_{n_1=0}^{1}\cdots\sum_{n_{N-1}=0}^{1}\frac{1}{\prod\limits_{i=1}^{N-1}(-p_i)^{n_i}}\left(1-\frac{1}{p_N}(q^d)^{\prod\limits_{i=1}^{N-1}p_i^{n_i}}\right)$$

Avec

$$\sum_{n_1=0}^{1}\cdots\sum_{n_{N-1}=0}^{1}\frac{1}{\prod\limits_{i=1}^{N-1}(-p_i)^{n_i}}=\prod_{i=1}^{N-1}\left(\sum_{n_i=0}^{1}\frac{1}{(-p_i)^{n_i}}\right)=\prod_{i=1}^{N-1}\left(1-\frac{1}{p_i}\right)$$

On obtient alors

$$A_N=\prod_{i=1}^{N-1}\left(1-\frac{1}{p_i}\right)-\frac{1}{p_N}\sum_{n_1=0}^{1}\cdots\sum_{n_{N-1}=0}^{1}\frac{(q^d)^{\prod\limits_{i=1}^{N-1}p_i^{n_i}}}{\prod\limits_{i=1}^{N-1}(-p_i)^{n_i}}=\prod_{i=1}^{N-1}\left(1-\frac{1}{p_i}\right)-\frac{1}{p_N}A_{N-1}$$

Par suite

$$(-1)^N\left(\prod_{i=1}^{N}p_i\right)A_N-(-1)^{N-1}\left(\prod_{i=1}^{N-1}p_i\right)A_{N-1}=(-1)^Np_N\prod_{i=1}^{N-1}(p_i-1)$$

Par sommation téléscopique, on obtient

$$(-1)^N\left(\prod_{i=1}^{N}p_i\right)A_N=-p_1A_1+\sum_{k=2}^{N}(-1)^kp_k\prod_{i=1}^{k-1}(p_i-1)$$

Or

$$p_1 A_1 = 2\sum_{n\in\{0,1\}} \frac{1}{(-2)^n}(q^d)^{2^n} = 2\left(1-\frac{1}{2}(q^d)^2\right) = 2-q^{2d}$$

D'où

$$A_N = \frac{(-1)^N}{\prod_{i=1}^{N} p_i}\left(q^{2d}-2-\sum_{k=2}^{N}(-1)^k p_k \prod_{i=1}^{k-1}(p_i-1)\right)$$

Enfin

$$\sum_{n_1,\ldots,n_N\in\mathbb{N}} \frac{1}{\prod_{i=1}^{N} p_i^{n_i}} \mu\left(\prod_{i=1}^{N} p_i^{n_i}\right)(q^d)^{\prod_{i=1}^{N} p_i^{n_i}} = \frac{(-1)^N}{\prod_{i=1}^{N} p_i}\left(q^{2d}-2-\sum_{k=2}^{N}(-1)^k p_k \prod_{i=1}^{k-1}(p_i-1)\right)$$

Avec

$$\left|\frac{(-1)^N}{\prod_{i=1}^{N} p_i}(q^{2d}-2)\right| \leqslant \frac{q^{2d}-2}{2^N} \underset{N\to+\infty}{\to} 0$$

Et

$$\left|\frac{(-1)^N}{\prod_{i=1}^{N} p_i}\sum_{k=2}^{N}(-1)^k p_k \prod_{i=1}^{k-1}(p_i-1)\right| \leqslant \sum_{k=2}^{N}\frac{1}{\prod_{i=k+1}^{N} p_i}\prod_{i=1}^{k-1}\left(1-\frac{1}{p_i}\right) \leqslant \sum_{k=2}^{N}\frac{1}{2^{N-k}} < 4 < +\infty$$

Par suite la limite de $\frac{(-1)^N}{\prod_{i=1}^{N} p_i}\left(q^{2d}-2-\sum_{k=2}^{N}(-1)^k p_k \prod_{i=1}^{k-1}(p_i-1)\right)$ existe lorsque N tend vers $+\infty$ existe et fini.

On a alors

$$\#\mathcal{P}_K(n) = \sum_{d=1}^{+\infty}\frac{1}{d}\left(\lim_{N\to+\infty}\frac{(-1)^N}{\prod_{i=1}^{N} p_i}\left(q^{2d}-2-\sum_{k=2}^{N}(-1)^k p_k \prod_{i=1}^{k-1}(p_i-1)\right)\right)$$

Ainsi

$$\#\mathcal{P}_K(n) = \sum_{d=1}^{+\infty}\frac{1}{d}\left(\lim_{N\to+\infty}\frac{(-1)^{N-1}}{\prod_{i=1}^{N} p_i}\sum_{k=2}^{N}(-1)^k p_k \prod_{i=1}^{k-1}(p_i-1)\right)$$

Or

$$\sum_{d=1}^{+\infty}\frac{1}{d}\left(\lim_{N\to+\infty}\frac{(-1)^{N-1}}{\prod_{i=1}^{N}p_i}\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)\right)=\alpha\sum_{d=1}^{+\infty}\frac{1}{d}=+\infty$$

Avec $\alpha=\lim_{N\to+\infty}\frac{(-1)^{N-1}}{\prod_{i=1}^{N}p_i}\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)$

Finalement, on a

$$\sum_{n=1}^{+\infty}(\#K-1).\#\mathcal{P}_K(n)=+\infty$$

Pour n'importe quel corps K commutatif et fini, il existe une infinité de polynômes irréductibles dans $K[X]$

Corollaire 2.

Pour tout entier $N\in\mathbb{N}^\star$, il existe une inifinité de polynômes irréductibles sur $K[X]$

Remarque 1.

On peut eviter tout ces calcules, et on montre tout simplement que

$$\#\mathcal{P}_K(n)\underset{n\to+\infty}{\sim}\frac{(\#K)^n}{n}$$

Puisque la série $\sum_{n>0}\frac{(\#K)^n}{n}$ est à terme positifs et divergente, alors

$$\sum_{n=1}^{+\infty}(\#K-1).\#\mathcal{P}_K(n)=+\infty$$

Référence:

agreg-maths.fr/uploads/versions/2055/Polyn%C3%B4mes%20irr%C3%A9ductibles%20sur%20Fq%20(123,125,141,190).pdf