Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

Corps finis

1 Corps finis

Lemme 1
Soit K un corps fini ; tout sous-anneau A de K est un corps.

$\triangledown$ Notons que A est intègre ; pour tout $x \in A \setminus \{0\}$, l'application :

$$\begin{aligned} m_x : A &\longrightarrow A \\ y &\longrightarrow xy \end{aligned}$$

est injective donc bijective puisque A est fini. En particulier x et inversible. $\triangle$
Considérons un corps fini K ; l'image de l'homomorphisme *caractéristique*

$$\begin{aligned} c_K : \mathbb{Z} &\longrightarrow K \\ k &\longrightarrow k\,1_K \end{aligned}$$

est le plus petit sous-anneau de K (le sous-corps *premier* de K) qui est donc isomorphe au corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; l'entier *premier* p est la caractéristique de K. Le sous-corps premier de K est encore l'ensemble $K^{\mathcal{F}_{K/\mathbb{F}_p}}$ des points fixes de l'automorphisme de Frobenius (*petit théorème de Fermat*) [1] :

$$\begin{aligned} \mathcal{F}_{K/\mathbb{F}_p} : K &\longrightarrow K \\ x &\longrightarrow x^p \end{aligned}$$

De plus K est canoniquement muni d'une structure de $\mathbb{F}_p$-espace vectoriel de dimension finie n. On a donc :

$$K \simeq (\mathbb{Z}/\mathbb{Z}p)^n \quad \text{et en particulier} \quad \mathrm{Card}(K) = p^n$$

La dimension n est le *degré* $n = [K : \mathbb{F}_p]$ de la $\mathbb{F}_p$-extension K.

Soit K un corps fini ayant q éléments ; pour tout entier $n \geq 1$, on désigne par $\mathrm{Irr}_K(n)$ l'ensemble des polynômes unitaires , irréductibles de degré n dans $K[X]$ et on pose :

$$\mathrm{I}_K(n) = \mathrm{Card}(\mathrm{Irr}_K(n))$$

Lemme 2
Pour tout entier $n \geq 1$, on a :

$$q^n = \sum_{d|n} d\,\mathrm{I}_K(d)$$

1. tout élément x du sous-corps premier vérifie $x^p = x$ donc est racine du polynôme $X^p - X$ et comme ce dernier possède p racines on a l'égalité

$\triangledown$ Pour tout entier $n \geq 0$, le nombre de polynômes *unitaires* de $K[X]$ de degré n est égal en q^n ; on regroupe ces nombres en une *série génératrice* :

$$\sum_{n=0}^{\infty} q^n \, T^n = \frac{1}{1 - q\,T} \in \mathbb{Z}[[T]]$$

Par ailleurs, tout polynôme unitaire $F \in K[X]$ de degré $n \geq 1$ s'écrit de manière unique $F = P_1^{k_1} \cdots P_r^{k_r}$ avec P_i unitaire, irréductible de degré $d_i \leq n$ pour $1 \leq i \leq r$, et l'on a $n = \sum_{i=1}^{r} k_i \, d_i$.
Pour $n \geq 1$, on considère la suite [2], ordonnée selon les degrés croissants, $P_1, \cdots, P_{r(n)}$ des polynômes unitaires, irréductibles de degré $\leq n$; le nombre de polynômes unitaires de degré $n \geq 0$ est ainsi le nombre de $r(n)$-uples $(k_1, \cdots, k_{r(n)})$ tels que [3] $n = \sum_{i=1}^{r(n)} k_i \, d_i$. C'est donc le coefficient de T^n dans le développement en série formelle du produit :

$$\frac{1}{1 - T^{d_1}} \cdots \frac{1}{1 - T^{d_{r(n)}}} = \prod_{d=1}^{n} \left(\frac{1}{1 - T^d} \right)^{\mathrm{I}_K(d)}$$

ou encore le coefficient de T^n dans le *produit infini* :

$$\prod_{d=1}^{\infty} \left(\frac{1}{1 - T^d} \right)^{\mathrm{I}_K(d)}$$

de sorte que l'on a finalement :

$$\prod_{d=1}^{\infty} \left(\frac{1}{1 - T^d} \right)^{\mathrm{I}_K(d)} = \frac{1}{1 - q\,T}$$

En prenant la *dérivée logarithmique* [4] des deux membres et en multipliant par T on obtient :

$$\sum_{d=1}^{\infty} d\,\mathrm{I}_K(d) \frac{T^d}{1 - T^d} = \frac{q\,T}{1 - q\,T}$$

Par identification des coefficients, on obtient le résultat. $\triangle$

Proposition 1
Pour tout entier $n \geq 1$, l'ensemble $\mathrm{Irr}_K(n)$ est non vide.

$\triangledown$ On a $q^n = \sum_{d|n} d\,\mathrm{I}_K(d)$.
On a alors, pour tout d :

$$q^d = \sum_{r|d} r \mathrm{I}_K(r) \geq d \mathrm{I}_K(d)$$

---

2. on a $r(n) = \sum_{d=1}^{n} \mathrm{I}_K(d)$.
3. $d_i = \deg(P_i)$ pour $1 \leq i \leq r(n)$
4. homomorphisme de groupes DL : $\mathbb{Z}[[T]]^{\times} \longrightarrow \mathbb{Z}[[T]]$ tel que $\mathrm{DL}(1 - X^n) = -nX^{n-1} + \cdots$ pour tout $n \geq 1$

par conséquent :

$$q^n = \sum_{d|n} d\mathrm{I}_K(d) = n\mathrm{I}_K(n) + \sum_{\substack{d|n \\ d\neq n}} d\mathrm{I}_K(d)$$

$$\leq n\mathrm{I}_K(n) + \sum_{\substack{d|n \\ d\neq n}} q^d \leq n\mathrm{I}_K(n) + \sum_{d=0}^{n-1} q^d \leq n\mathrm{I}_K(n) + \frac{q^n-1}{q-1}$$

d'où [5]

$$n\mathrm{I}_K(n) \geq q^n - \frac{q^n-1}{q-1} \geq 1$$

et finalement $\mathrm{I}_K(n) \geq 1$. $\triangle$

Corollaire 1
Pour tout entier premier p et tout $n \in \mathbb{N}^*$, il existe un corps fini K ayant p^n éléments [6].

$\triangledown$ Pour tout entier premier p et tout $n \in \mathbb{N}^*$, il existe un polynôme unitaire irréductible $P \in \mathbb{F}_p[X]$ de degré n ; alors $K = \mathbb{F}_p[X]/(P)$ est un corps et un $\mathbb{F}_p$ espace vectoriel de dimension n donc K est fini et possède p^n éléments. On a $K = \mathbb{F}_p[x]$ où $x = \overline{X}$ et $p_{x,\mathbb{F}_p} = P$.
$\triangle$.

Lemme 3
Soit K un corps fini ayant $q = p^n$ éléments ; alors le groupe multiplicatif $K^\star$ est cyclique d'ordre $q-1$:

$$K^\star \simeq \mathbb{Z}/\mathbb{Z}(q-1)$$

$\triangledown$ Le groupe abélien fini $K^\star$ est d'*ordre* $q-1$ et d'*exposant* [7] e. L'ordre de chaque élément de $K^\star$ divise e et il existe un élément $x \in K^\star$ qui est d'ordre e.
On a donc $z^e = 1$ pour tout $z \in K^\star$, donc $z^{e+1} - z = 0$ pour tout $z \in K$.
Mais e divise $q-1$, donc $e \leq q-1$. Si l'on avait $e+1 < q$, le polynôme $Z^{e+1} - Z \in \mathbb{F}_p$ possèderait q racines dans K ce qui n'est pas possible. On a donc $e = q-1$ et x est un générateur de $K^\star$. $\triangle$

---

5. on a $q \geq 2$

6. Plus généralement, pour tout corps fini K avec $\mathrm{Card}(K) = q$, il existe une K-extension L avec $\mathrm{Card}(L) = q^n$. On peut étendre à ce cadre les résultats de ce chapitre.

7. l'exposant d'un groupe abélien fini est le plus grand de ses facteurs invariants. On peut aussi l'introduire de manière plus élémentaire de la manière suivante :

✓ *Soient x, y des éléments d'ordre finis $m = o(x)$ et $n = o(y)$ d'un groupe G tels que $xy = yx$; si m et n sont premiers entre eux, alors xy est d'ordre $o(xy) = mn$.*
$\triangledown$ On a évidemment $(xy)^{mn} = (x^m)^n (y^n)^m = 1$ de sorte que $o(xy)$ divise mn.
Supposons que $(xy)^h = 1$ de sorte que $x^h = y^{-h} \in < x > \cap < y >$. Puisque m et n sont premiers entre eux, on a $< x > \cap < y > = \{1\}$, m et n divisent h ; alors mn divise h et xy est d'ordre mn. $\triangle$

✓ *Soient x, y des éléments d'ordre finis $m = o(x)$ et $n = o(y)$ d'un groupe G tels que $xy = yx$; alors il existe un élément z dans le sous-groupe $< x, y >$ de G engendré par x et y dont l'ordre est $o(z) = \mathrm{ppcm}(m, n)$.*
$\triangledown$ On a $m = p_1^{a_1} \cdots p_r^{a_r} p_{r+1}^{a_{r+1}} \cdots p_{r+s}^{a_{r+s}}$ et $n = p_1^{b_1} \cdots p_r^{b_r} p_{r+1}^{b_{r+1}} \cdots p_{r+s}^{b_{r+s}}$ avec $a_i \geq b_i$ pour $1 \leq i \leq r$ et $a_{r+j} < b_{r+j}$ pour $1 \leq j \leq s$.
Posons $m' = p_1^{a_1} \cdots p_r^{a_r}$ et $n' = p_{r+1}^{b_{r+1}} \cdots p_{r+s}^{b_{r+s}}$. Alors $x^{m/m'}$ est d'ordre m' et $y^{n/n'}$ est d'ordre n' de sorte que $z = x^{m/m'} y^{n/n'}$ est d'ordre $m'n' = \mathrm{ppcm}(m, n)$. $\triangle$

✓ *Soit G un groupe abélien fini et e le maximum des ordres des éléments de G. Alors e divise l'ordre de G et est égal au ppcm des ordres des éléments de G.* $\triangledown$ Soit $x \in G$ un élément d'ordre maximal $o(x) = e$; pour tout $y \in G$ d'ordre $o(y)$, il existe un élément $z \in < x, y >$ tel que $o(z) = \mathrm{ppcm}(e, o(y))$. Puisque e est maximal on a $o(z) = e$ de sorte que $o(y)$ divise e. $\triangle$

Corollaire 2 (théorème de l'élément primitif)
Soit K un corps fini ayant $q = p^n$ éléments ; il existe $x \in K$ tel que $K = \mathbb{F}_p[x]$. En particulier on a $K \simeq \mathbb{F}_p[X]/\langle P \rangle$ avec $P = p_{x,\mathbb{F}_p}$ unitaire, irréductible de degré n

$\triangledown$ il suffit de prendre pour x un générateur [8] du groupe $K^\star$. $\triangle$

Corollaire 3
Soit K un corps fini ayant $q = p^n$ éléments ; l'automorphisme de Frobenius $\mathcal{F}_{K/\mathbb{F}_p}$ est d'ordre n.

$\triangledown$ On a $\mathcal{F}^n_{K/\mathbb{F}_p} = \mathrm{id}$. Soit x un générateur de $K^\star$ si $\mathcal{F}^k_{K/\mathbb{F}_p} = \mathrm{id}$ on a $\mathcal{F}^k_{K/\mathbb{F}_p}(x) = x$ de sorte que $x^{p^k} - 1 = 0$ donc $q - 1 = p^n - 1 | p^k - 1$ et finalement [9] $n|k$. $\triangle$

Lemme 4
Tout polynôme irréductible $P \in \mathbb{F}_p[X]$ est sans facteurs multiples.

$\triangledown$ Posons $\Delta = \mathrm{pgcd}(P, P')$. Supposons que P ait un facteur multiple de sorte que $\deg(\Delta) \geq 1$. Mais P étant irréductible , Δ et P sont associées ; P divise alors P' de sorte que $P' = 0$. Dans ce cas on a $P = a_r X^{rp} + \cdots + a_1 X^p + a_0$ avec $a_i \in \mathbb{F}_p[X]$, donc $a_i = a_i^p$, pour $0 \leq i \leq n$. On a ainsi $P = (a_r X^r + \cdots + a_1 X + a_0)^p$ et P ne serait pas irréductible. $\triangle$

Lemme 5
Soit K un corps fini ayant $q = p^n$ éléments ; tout polynôme irréductible $P \in \mathbb{F}_p[X]$ qui possède une racine x dans K possède toutes ses racines dans K (ie. la $\mathbb{F}_p$-extension K est galoisienne).

$\triangledown$ Pour $P \in \mathbb{F}_p[X]$ unitaire et irréductible, soit $\mathcal{R} = \{y \in K / P(y) = 0\}$ l'ensemble de ses racines dans K ; on a $x \in R$. On considère le polynôme $Q = \prod_{y \in \mathcal{R}} (X - y) \in K[X]$. On a $\mathcal{F}_{K/\mathbb{F}_p}(\mathcal{R}) = \mathcal{R}$ d'où $\mathcal{F}_{K/\mathbb{F}_p}(Q) = Q$ de sorte que, d'après le *petit théorème de Fermat*, $Q \in \mathbb{F}_p[X]$ et par suite $Q = P$ puisque $Q|P$. Ainsi toutes les racines de P sont dans K. $\triangle$

---

8. Attention ! un élément primitif de la $\mathbb{F}_p$-extension K ie. tel que $K = \mathbb{F}_p[x]$ n'est pas nécessairement un générateur du groupe $K^\star$

9. Soient m et n deux entiers naturels ; les conditions suivantes sont équivalentes :

i. m divise n

ii. $p^m - 1$ divise $p^n - 1$

iii. $X^{p^m} - X$ divise $X^{p^n} - X$

$\triangledown$ Ecrivons $n = mq + r$ avec $0 \leq r \leq m - 1$; on a

$$\begin{aligned} p^n - 1 &= p^{mq+r} - 1 \\ &= (p^{mq} - 1)p^r + (p^r - 1) \\ &= (p^m - 1)\underbrace{p^r((p^m)^{q-1} + \cdots + p^m + 1)}_{=h} + (p^r - 1) \end{aligned}$$

de sorte que m divise n si et seulement si $p^m - 1$ divise $p^n - 1$.
De même on a

$$\begin{aligned} X^{p^n-1} - 1 &= X^{(p^m-1)h} X^{p^r-1} - 1 \\ &= (X^{(p^m-1)h} - 1)X^{p^r-1} + X^{p^r-1} - 1 \\ &= (X^{p^m-1} - 1)((X^{p^m-1})^{h-1} + \cdots + X^{p^m-1} + 1)X^{p^r-1} + X^{p^r-1} - 1 \\ &= X^{p^n-1} - 1 = (X^{p^m-1} - 1)\,Q + (X^{p^r-1} - 1) \end{aligned}$$

$\triangle$

Lemme 6
Soit K un corps fini ayant $q = p^n$ éléments ; on considère un polynôme irréductible unitaire $P \in \mathbb{F}_p[X]$ de degré m possédant une racine x dans K ; on a $m|n$ et l'ensemble des racines de P dans K est $Z(P) = \{x, x^p, \cdots, x^{p^{m-1}}\}$. De plus $P|X^{p^m} - X$.

$\triangledown$ $\mathbb{F}_p[x]$ est une sous-extension de K *canoniquement isomorphe* à $\mathbb{F}_p[X]/\langle P\rangle$ donc de degré m et par *multiplicativité des degrés* on a $m|n$. Par ailleurs :

$$\begin{array}{rccc} \mathcal{F}_{\mathbb{F}_p[x]/\mathbb{F}_p} : \mathbb{F}_p[x] & \longrightarrow & \mathbb{F}_p[x] \\ y & \longrightarrow & y^p \end{array}$$

est d'ordre [10] m de sorte que les $x_i = x^{p^i} \in \mathbb{F}_p[x]$, $0 \leq i \leq m-1$ de P sont deux à deux distincts et racines de P.
De plus, si $x \neq 0$ (*ie.* $P \neq X$), puisque le groupe $\mathbb{F}_p[x]^\star$ est d'ordre $p^m - 1$, on a $x_i^{p^m-1} = 1$ pour $0 \leq i \leq m-1$ et $P|X^{p^m-1} - 1$. $\triangle$

Lemme 7
Soit K un corps fini ayant p^n éléments, pour L corps fini, il existe un morphisme $\varphi : K \longrightarrow L$ si et seulement si L est de caractéristique p et $n|[L : \mathbb{F}_p]$. Dans ces conditions, $\varphi(K) = L^{\mathcal{F}^n_{L/\mathbb{F}_p}}$ est l'unique sous-corps de L ayant p^n éléments

$\triangledown$ S'il existe un morphisme $\varphi : K \longrightarrow L$, φ est injectif donc K et L sont de même caractéristique p et $\varphi(K)$ est un sous-corps de L *isomorphe* à K. Alors [11] $K^\star$ est isomorphe à un sous-groupe de $L^\star$ d'où $p^n - 1|p^N - 1$ où $\mathrm{Card}(L) = p^N$ et $n|N$.
Réciproquement supposons que $n|N$; on a, par le théorème de l'élément primitif $K = \mathbb{F}_p[x]$. Or L est *l'ensemble* des racines du polynôme $X^{p^N} - X$; comme $P = p_{x,\mathbb{F}_p}$ divise $X^{p^n} - X$ donc divise $X^{p^N} - X$, P possède une racine $y \in L$ de sorte qu'il existe un unique homomorphisme $\varphi : K \longrightarrow L$ tel que $\varphi(x) = y$.
Enfin si K' étant un sous-corps de L ayant p^n éléments, K' est l'ensemble des racines de $X^{p^n} - X$ donc est égal à $L^{\mathcal{F}^n_{L/\mathbb{F}_p}}$. $\triangle$.

Corollaire 4
Deux corps finis K et L sont isomorphes si et seulement s'ils ont même caractéristique et même degré (ie. si et seulement si $\mathrm{Card}(K) = \mathrm{Card}(L)$*).*

$\triangledown$ Supposons que $\mathrm{Card}(K) = \mathrm{Card}(L)$, il existe un morphisme $\varphi : K \longrightarrow L$ qui est nécessairement injectif, et par cardinalité, qui est surjectif. $\triangle$.

2 Polynômes cyclotomiques

Soit p premier ; on considère un entier n tel que p *ne divise pas* n et on désigne par m *l'ordre* de $\overline{p}$ dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments *inversibles* de l'anneau $\mathbb{Z}/n\mathbb{Z}$. On a $m|\varphi(n)$ et le polynôme $X^n - 1 \in \mathbb{F}_p[X]$ est *sans facteur multiple.*
On désigne par K un corps fini ayant p^m éléments.
L'ensemble des racines de $X^n - 1$ dans K forme l'*unique* sous-groupe [12] $\mu_n(K)$ d'ordre n de $K^\star$; ce groupe $\mu_n(K)$ est cyclique d'ordre n. On notera $\Pi_n(K)$ l'ensemble des générateurs de $\mu_n(K)$; on a :

$$\mathrm{Card}(\Pi_n(K)) = \varphi(n) \quad \text{et} \quad \mathcal{F}_{K/\mathbb{F}_p}(\Pi_n(K)) = \Pi_n(K)$$

10. comme $\mathcal{F}^n_{\mathbb{F}_p[x]/\mathbb{F}_p} = \mathrm{id}|_{\mathbb{F}_p[x]}$ on retrouve que $m|n$
11. on peut aussi utiliser la multiplicativité des degrés $[L : \mathbb{F}_p] = [L : \varphi(K)]\,[\varphi(K) : \mathbb{F}_p]$
12. puisque le groupe $K^\star$ est *cyclique* d'ordre $p^m - 1$ et que $n|p^m - 1$

Par ailleurs, soit :

$$\mu_n(\mathbb{C}) = \{e^{k\frac{2\pi i}{n}} \,/\, 0 \leq k \leq n-1\}$$

le groupe cyclique d'ordre n des racines $n^{\text{èmes}}$ de l'unité dans $\mathbb{C}$; l'ensemble de ses générateurs :

$$\Pi_n(\mathbb{C}) = \{e^{k\frac{2\pi i}{n}} \,/\, 0 \leq k \leq n-1, k \text{ premier avec } n\}$$

permet de définir le polynôme cyclotomique

$$\Phi_n = \prod_{z \in \Pi_n(\mathbb{C})} (X - z) \in \mathbb{Z}[X]$$

On a $\Phi_n \in \mathbb{Z}[X]$ unitaire, irréductible et de degré $\varphi(n)$. On a alors la décomposition en facteurs irréductibles :

$$X^n - 1 = \prod_{d|n} \Phi_d$$

Considérons $\overline{\Phi_n} \in \mathbb{F}_p[X]$ la réduction modulo p du polynôme cyclotomique $\Phi_n \in \mathbb{Z}[X]$ qui est évidemment unitaire et de degré $\varphi(n)$;

Lemme 8
On a

$$\overline{\Phi_n} = \prod_{x \in \Pi_n(K)} (X - x) \in K[X]$$

$\triangledown$ On a dans $\mathbb{F}_p[X]$ (p premier ne divisant pas n) :

$$X^n - 1 = \prod_{d|n} \overline{\Phi_d}$$

Ainsi tout $x \in \Pi_n(K)$ est racine de l'un des polynômes $\overline{\Phi_d}$, mais comme $\overline{\Phi_d}$ divise $X^d - 1$ et que x est d'ordre n, il en résulte que x est racine de $\overline{\Phi_n}$.
Ainsi, comme $\overline{\Phi_n}$ est degré $\varphi(n)$ et sans facteurs multiples, dans $K[X]$, on obtient le résultat. $\triangle$

Lemme 9
Pour tout $x \in \Pi_n(K)$, le polynôme minimal $p_{x,\mathbb{F}_p} \in \mathbb{F}_p[X]$ de $x \in \Pi_n(K)$ est un facteur irréductible de degré m de $\overline{\Phi_n}$ de sorte que[13] *$K = \mathbb{F}_p[x]$ et l'ensemble :*

$$Z(p_{x,\mathbb{F}_p}) = \{x, x^p, \cdots, x^{p^{m-1}}\}$$

de ses racines dans K est un cycle de la permutation $\mathcal{F}_{K/\mathbb{F}_p}$ de $\Pi_n(K)$.

$\triangledown$ Considérons la sous-$\mathbb{F}_p$-extension $\mathbb{F}_p[x] \subset K$ et posons :

$$m' = \deg(p_{x,\mathbb{F}_p}) = [\mathbb{F}_p[x] : \mathbb{F}_p]$$

On a $x \in \mathbb{F}_p[x]^\star$ et comme x est d'ordre n on a $n|p^{m'} - 1$ de sorte que $m|m'$.
Mais on a $\mathbb{F}_p[x]^\star \subset K^\star$ donc $p^{m'} - 1|p^m - 1$ d'où $m'|m$, $m' = m$ et $\mathbb{F}_p[x] = K$.
Ainsi x est racine dans K du polynôme irréductible $p_{x,\mathbb{F}_p}$ qui est de degré m de sorte que $Z(p_{x,\mathbb{F}_p}) = \{x, x^p, \cdots, x^{p^{m-1}}\}$ avec $(x^{p^{m-1}})^p = x^{p^m} = x$. $\triangle$

13. K est ainsi l'analogue en caractéristique p du corps cyclotomique $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$

Corollaire 5
$\overline{\Phi_n}$ se décompose dans $\mathbb{F}_p[X]$ en un produit de $\dfrac{\varphi(n)}{m}$ polynômes unitaires irréductibles distincts de degré m correspondant à la décomposition[14] *en cycles à support disjoints de la permutation $\mathcal{F}_{K/\mathbb{F}_p}$ de $\Pi_n(K)$.*

$\triangledown$ Pour tout $x \in \Pi_n(K)$, les racines de $p_{x,\mathbb{F}_p}$ sont les $x^{p^i}\Pi_n(K)$ pour $0 \leq i \leq m-1$ de sorte que $p_{x,\mathbb{F}_p}$ est l'un des facteurs irréductibles de $\overline{\Phi_n}$ dans $\mathbb{F}_p[X]$.
Réciproquement soit $P \in \mathbb{F}_p[X]$ un facteur irréductible (unitaire) de $\overline{\Phi_n}$; il existe $x \in \Pi_n(K)$ tel que $P(x) = 0$ donc $p_{x,\mathbb{F}_p}|P$ et comme P est irréductible on a $P = p_{x,\mathbb{F}_p}$.
Enfin $p_{x,\mathbb{F}_p} = p_{x',\mathbb{F}_p}$ si et seulement s'ils ont les mêmes racines ce qui revient à dire que x et x' sont dans le même cycle de la permutation $\mathcal{F}_{K/\mathbb{F}_p}$ de $\Pi_n(K)$. $\triangle$

Corollaire 6
Les polynômes $P \in \mathbb{F}_p[X]$ unitaires, irréductibles tels que $x = \overline{X}$ soit d'ordre n dans $K^\star$ où $K = \mathbb{F}_p[X]/\langle P\rangle = \mathbb{F}_p[x]$ sont les facteurs irréductibles de $\overline{\Phi_n}$. En particulier $\deg(P) = [\mathbb{F}_p[x] : \mathbb{F}_p]$ *est l'ordre m de $\overline{p}$ dans $(\mathbb{Z}/\mathbb{Z}n)^\times$.*

$\triangledown$ On a $P = p_{x,\mathbb{F}_p}$ et x d'ordre n de sorte $P|\overline{\Phi_n}$. Il en résulte que $\deg(P) = m$. $\triangle$

Etant donné $P \in \mathrm{Irr}_p(m)$ et $K = \mathbb{F}_p[X]/P\mathbb{F}_p[X] = \mathbb{F}_p[x]$ où $x = \overline{X}$. Tout élément de $a \in K$ s'écrit alors de manière unique $a = \sum_{i=0}^{m-1} a_i x^i$ avec $a_i \in \mathbb{F}_p$ pour $0 \leq i \leq m-1$. (*représentation additive* des éléments de K).
Pour $a = \sum_{i=0}^{m-1} a_i x^i, b = \sum_{i=0}^{m-1} b_i x^i$ on a $a + b = \sum_{i=0}^{m-1} (a_i + b_i)x^i$. Par contre on a $ab = \sum_{i=0}^{m-1} c_i x^i$ où $R = \sum_{i=0}^{m-1} c_i X^i$ est le reste de la division euclidienne par le polynôme minimal P du produit $(\sum_{i=0}^{m-1} a_i X^i)(\sum_{j=0}^{m-1} b_j X^j)$.
Les polynômes $P \in \mathrm{Irr}_p(m)$ pour lesquels la *racine symbolique* x est un générateur du groupe cyclique $K^\star$ sont appelés les polynômes *primitifs*. Ce sont ceux pour lesquels $n = p^m - 1$ *ie.* les facteur irréductibles P de $\overline{\Phi_{p^m-1}}$. Dans ces conditions tout élément $a \in K^\star$ s'écrit de manière unique $a = x^k$ avec $k \in \mathbb{Z}/(p^m-1)\mathbb{Z}$ (*représentation multiplicative*). On obtient ainsi un isomorphisme de groupes :

$$\begin{array}{rccc} \mathrm{LD}_x : & K^\star & \longrightarrow & \mathbb{Z}/(p^m-1)\mathbb{Z} \\ & a = x^k & \longrightarrow & k = \log_x(a) \end{array}$$

appelé *logarithme discret* de base x.

14. qui est formée de $\dfrac{\varphi(n)}{m}$ m-cycles