Développement 1 : Facteurs irréductibles de $X^q - X$

Soit p un entier premier et $q = p^n$.

Lemme 1 : Soit P un polynôme irréductible de degré n sur $\mathbb{F}_p$. Alors P divise $X^q - X$ dans $\mathbb{F}_p[X]$ donc est scindé dans $\mathbb{F}_q$; donc $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ est son corps de décomposition.

Démonstration : Soit P un polynôme irréductible de degré n.
Si $P(X) \neq X$, soit L un corps de décomposition de $P(X)$ sur $\mathbb{F}_p$ et soit θ une racine de $P(X)$ dans L.
Alors $\mathbb{F}_p(\theta) \simeq \mathbb{F}_p[X]/(P) \simeq \mathbb{F}_q$.
Donc $\theta^{q-1} = 1$, donc $P \mid X^q - X$ dans $\mathbb{F}_p[X]$.

Théorème : On note $\mathcal{K}(p,d)$ l'ensemble des polynômes irréductibles unitaires de degré d sur $\mathbb{F}_p$.
Alors $X^q - X = \prod_{d \mid n} \prod_{Q \in \mathcal{K}(p,d)} Q(X)$.

Schéma de la démonstration :

1) Si d diviseur de n, on montre que tout $Q \in \mathcal{K}(p,d)$ divise $X^q - X$. et que les éléments de $\mathcal{K}(p,d)$ sont premiers entre eux.

2) On note alors $X^q - X = H(X) \prod_{d \mid n} \prod_{Q \in \mathcal{K}(p,d)} Q(X)$. ; on suppose par l'absurde que $\deg(H) \geq 1$.
→ on montre que si F est un facteur irréductible de H alors F^2 divise $X^q - X$; absurde ; d'où la conclusion...

---

1) Soit $d \mid n$. On a alors $p^d - 1 \mid p^n - 1$
(en effet $p^n - 1 = p^{kd} - 1 = (p^d - 1)(p^{(k-1)d} + \cdots + p^d + 1)$)
Donc de même $X^{p^d-1} - 1 \mid X^{p^n-1} - 1 = X^{q-1} - 1$.
Or d'après le lemme, tout élément Q de $\mathcal{K}(p,d)$ divise $X^{p^d-1} - 1$ (sauf pour $\mathcal{K}(p,1) = \{X\}$) Donc tout élément Q de $\mathcal{K}(p,d)$ divise $X^q - X$. Les éléments de $\mathcal{K}(p,d)$ pour $d \mid n$ étant premiers entre eux deux à deux, on a :

$$\prod_{d \mid n} \prod_{Q \in \mathcal{K}(p,d)} Q(X) \mid X^q - X.$$

2) On note donc $X^q - X = H(X) \prod_{d|n} \prod_{Q \in \mathcal{N}(p,d)} Q(X)$.

On suppose $\deg(H) \geq 1$.
Soit F un facteur irréductible de H et $d = \deg(F)$.
Alors $F \mid X^q - X$ et d'autre part $F \mid X^{p^d} - X$ (par le lemme)
Donc $F \mid (X^{p^n} - X) \wedge (X^{p^d} - X) = X((X^{p^n-1} - 1) \wedge (X^{p^d-1} - 1))$

$$= X(X^{(p^n-1)\wedge(p^d-1)} - 1)$$

$$= X(X^{p^{d\wedge n}-1} - 1).$$

(En effet, pour tout anneau commutatif unitaire intègre A et $a \in A \setminus A^\times$ on a pour tous $u, v \in \mathbb{N}^*$: $(u \mid v) \Leftrightarrow a^u - 1 \mid a^v - 1$)

Donc $F \mid \Delta(X) = X^{p^\delta} - X$ où $\delta = d \wedge n$.
$\Delta(X)$ est un polynôme de degré p^δ à coefficients dans $\mathbb{F}_p$.
Donc admet p^d racines dans $\mathbb{F}_{p^d} \simeq \mathbb{F}_p[X]/(F)$.
Donc $p^d \leq p^\delta$, donc $\left.\begin{matrix} d \leq \delta \\ \delta \mid d \end{matrix}\right\}$; donc $d = \delta$; donc $d \mid n$

$\Rightarrow F(X) \in \mathcal{N}(p,d)$, $d \mid n$ donc $F(X)^2 \mid X^{p^n} - X$ dans $\mathbb{F}_p[X]$.
Ce qui est absurde puisque $X^q - X$ est sans facteur carré.
Donc $\deg(H) = 0$ et donc $X^q - X = \prod_{d|n} \prod_{Q \in \mathcal{N}(p,d)} Q(X)$.