Se ramener à un produit de facteurs inéductibles de même degré

Cf Demazure p237 "Cours d'algèbre" éd. Cassini.

On s'intéresse ici à des polynômes sur des corps finis.
On cherche à se ramener d'un polynôme P à un produit de R_i tel que chaque R_i soit un produit de facteurs inéductibles de même degré. On supposera ici P sans facteurs multiples, car on peut s'y ramener d'après 96.
Cette réduction est utile pour se ramener à des polynômes sur lesquels l'algorithme de Canto-Zassenhaus fonctionne. Cf 99.

97.1 Lemme Soit p un entier premier. Soit $m \in \mathbb{N}^*$. On pose $q = p^m$. Soit $n \in \mathbb{N}^*$
Dans $\mathbb{F}_q[X]$, $X^{q^n} - X$ est exactement le produit de tous les polynômes inéductibles unitaires dont le degré divise n

Preuve Soit $P \in \mathbb{F}_q[X]$ un polynôme inéductible unitaire, de degré r.
On note $\mathbb{K} = \mathbb{F}_q[X]/(P)$ et $\alpha = \overline{X}^{(P)}$ la classe de X modulo (P).
Rappelons que puisque $\deg(P) = r$, $\mathbb{K}$ est de cardinal q^r.

- Si $r \mid n$ disons $n = rk$.
On a $\alpha^{q^r} = \alpha$ ($\alpha^{q^r - 1} = 1$ car $o(\alpha) \mid \#\mathbb{K}^\times = q^r - 1$ par th de Lagrange).
En itérant k fois obtient $\alpha^{(q^r)^k} = \alpha$ soit $\alpha^{q^n} = \alpha$.
Cela s'écrit aussi $\overline{X}^{(P)\,q^n} - \overline{X}^{(P)} = 0$ donc $\overline{X^{q^n} - X}^{(P)} = 0$ donc $P \mid X^{q^n} - X$
- Si $P \mid X^{q^n} - X$
On a bien $\alpha^{q^n} = \alpha$ donc $\alpha \in A := \{a \in \mathbb{K},\ a^{q^n} = a\}$
A est un sous anneau de $\mathbb{K}$ (en tant que noyau de $F^{n \times m} - id_{\mathbb{K}}$ où $F = \left(\begin{smallmatrix} \mathbb{K} \to \mathbb{K} \\ x \mapsto x^p \end{smallmatrix}\right)$ le Frobenius)
Or $\alpha = \overline{X}^{(P)}$ engendre $\mathbb{K}$ donc $A = \mathbb{K}$, sinon $\dots$
$\mathbb{K}^\times$ est le gpe multiplicatif d'un corps fini, il est donc monogène (cf).
Il existe donc $g \in \mathbb{K}^\times$ tel que $o(g) = \#\mathbb{K}^\times = q^r - 1$. Mais puisque $g \in \mathbb{K} = A$
on a aussi $g^{q^n} = g$ donc $o(g) \mid q^n - 1$ soit $q^r - 1 \mid q^n - 1$ donc $r \mid n$
(donc $g^{q^n - 1} = 1$)

Soit $P \in \mathbb{F}_q[X]$ un polynôme unitaire sans facteurs multiples
On considère sa DFI (décomposition en facteurs irréductibles)
$P = \prod_{i=1}^{\hat{}} P_i$. On a alors $P = \prod_{j=1}^{n} R_j$. où $R_j = \prod_{i=1 \atop \deg P_i = j}^{\hat{}} P_i$ où $n = \deg(P)$
Chaque R_j est le produit de polynômes irréductibles de mêmes degrés, on a donc ici une factorisation répondant au problème mais elle est théorique. Montrons comment la calculer :

Pté . $\forall j \in [1..n]$ $\quad PGCD(P, X^{q^j} - X) = \prod_{k=1 \atop k|j}^{n} R_k$ (1)

. $\forall j \in [1..n]$ $\quad R_j = \left(\frac{PGCD(P, X^{q^j} - X)}{\prod_{k|j \atop k \neq j} R_k} \right)$ (2).

Preuve Le PGCD en question doit diviser P donc s'écrit comme produit de certains P_i, or on sait d'après le lemme que les seuls diviseurs de $X^{q^j} - X$ sont les irréductibles de degré divisant j, on en déduit que $PGCD(P, X^{q^j} - X) = \prod_{i=1 \atop \deg(P_i) | j}^{\hat{}} P_i$ ce qui en réorganisant les facteurs par mêmes degrés $PGCD(P, X^{q^j} - X) = \prod_{k=1 \atop k|j}^{n} \prod_{\deg(P_i) = k}^{\hat{}} P_i = \prod_{k=1 \atop k|j}^{n} R_k$.
D'où (1).
Cela donne aussi $PGCD(P, X^{q^j} - X) = \prod_{k|j \atop k \neq j} R_k \times R_j$ d'où (2).

On en déduit l'algorithme suivant.

Réduction_en_degré(P) :

$m = \deg(P)$. $i = 1$.
tant que $i \leq m$
calculer $Q = PGCD(P, X^{q^i} - X)$
si i premier, alors stocker $R_i = Q$
sinon stocker $R_i = Q / \prod_{j|i \atop j \neq i} R_j$
faire $m := \frac{m}{\deg(R_i)}$

Rq Grâce à cet algorithme on connaît aussi le degré de ses facteurs irréductibles.