Se ramener à un polynôme sans facteur multiple.

Objectif Agrégé p 247-248.
Demazure, Cours d'algèbre p 231-232.

On s'intéresse ici à des polynômes sur des corps finis. (ou du moins de caract $\neq 0$)
On cherche à se ramener d'un polynôme P à un produit de polynômes R_i tel que chaque R_i soit produit d'irréductibles deux à deux distincts.
Cette réduction est utile pour se ramener à des polynômes sur lesquels l'algorithme de Berlekamp fonctionne (Cf 98).

Soit p un nombre premier. Soit $\mathbb{K}$ un corps de caractéristique p.
Soit $P \in \mathbb{K}[X]$ unitaire. On considère $\prod_{i=1}^{s} P_i^{\alpha_i}$ sa décomposition en facteurs irréductibles (ie $\forall i \in [\![1..s]\!]$ $P_i \in \mathbb{K}[X]$ irréductible, $\alpha_i \in \mathbb{N}^*$ et les $(P_i)_{i \in [\![1..s]\!]}$ 2à2 $\neq$).

96.1 **Déf** P est dit sans facteur multiple $\iff \forall i \in [\![1..s]\!]$ $\alpha_i = 1$.

96.2 **Pté** $PGCD(P, P') = \prod_{i=1}^{s} P_i^{\beta_i}$ où $\forall i \in [\![1..s]\!]$ $\beta_i = \begin{cases} \alpha_i \text{ si } \alpha_i \cdot 1_{\mathbb{K}} = 0 \\ \alpha_i - 1 \text{ sinon} \end{cases}$

Preuve $P = \prod_{i=1}^{s} P_i^{\alpha_i}$ donc $P' = \sum_{j=1}^{s} \left(\prod_{\substack{i=1 \\ i \neq j}}^{s} P_i^{\alpha_i} \right) \times \alpha_j P_j' P_j^{\alpha_j - 1}$

$$= \underbrace{\sum_{j=1}^{s} \left(\alpha_j \times \prod_{\substack{i=1 \\ i \neq j}}^{s} P_i \times P_j' \right)}_{:= Q} \times \underbrace{\prod_{i=1}^{s} P_i^{\alpha_i - 1}}_{\text{divise } P.}$$

$\forall j \in [\![1..s]\!]$ $P_j \mid Q$ ssi $\alpha_j \cdot 1_{\mathbb{K}} = 0$ (sinon le j-ième terme de la somme qui fait apparaître du P_j' au lieu de P_j est le seul non divisible par P_j)
donc $\forall j \in [\![1..s]\!]$ $P_j^{\alpha_j} \mid P'$ ssi $\alpha_j \cdot 1_{\mathbb{K}} = 0$
A en tant que diviseur de P on sait que le $PGCD(P, P')$ s'écrit comme produit de certain des P_i, en fait comme produit de ceux des P_i qui divisent P'. On a donc $PGCD(P, Q) = \prod_{\substack{i=1 \\ \alpha_i \cdot 1_{\mathbb{K}} = 0}}^{s} P_i^{\alpha_i} \times \prod_{\substack{i=1 \\ \alpha_i \cdot 1_{\mathbb{K}} \neq 0}}^{s} P_i^{\alpha_i - 1}$

Donc $PGCD(P, P') = \prod_{i=1}^{s} P_i^{\beta_i}$ comme énoncé

96.3 **Cor** P est sans facteurs multiple $\iff PGCD(P, P') = 1$
En effet $PGCD(P, P') = 1$ ssi $\forall i \in [\![1..s]\!]$ $\beta_i = 0$ ssi $\forall i \in [\![1..s]\!]$ $\alpha_i = 1$ (et $\alpha_i \cdot 1_{\mathbb{K}} \neq 0$ évident)
(car $\alpha_i > 0$)

Le calcul du PGCD de P et P' est un calcul effectif qui se fait grâce à l'algorithme d'Euclide.
Il fournit une factorisation de P (en $P = PGCD(P,P') \times P/PGCD(P,P')$)
On aimerait pouvoir itérer sur chacun des sous-problèmes c-à-d chacun des facteurs fournis par cette décomposition, mais cela n'a un intérêt que si cette factorisation n'est pas triviale c-à-d si $PGCD(P,P') \neq P$. (Si $PGCD(P,P') = 1$ on a fini !).
Traitons donc ce cas :

Ptié Si $\mathbb{K}$ est un corps fini de caractéristique p et si $P \in \mathbb{K}[X]$ alors $PGCD(P,P') = P \iff P' = 0$
$\iff \exists \tilde{P} \in \mathbb{K}[X],\ P(X) = \tilde{P}(X^p)$
$\iff \exists R \in \mathbb{K}[X]\ \ P(X) = R(X)^p$
Et dans ce cas on sait calculer R à partir de P

Preuve • Si $PGCD(P,P') = P$ alors $P \mid P'$ donc $P' = 0$ ou $\deg(P) \leq \deg(P')$.
Or sauf pour $P = 0$ (qui implique $P' = 0$) $\deg(P') < \deg(P)$.
On a donc ici nécessairement $P' = 0$. La réciproque est claire car P est le plus grand diviseur de P et il divise aussi 0.

• On écrit $P = \sum_{i=0}^{d} a_i X^i$ $\quad P' = \sum_{i=0}^{d} i.a_i X^{i-1}$
$P' = 0 \iff \forall i \in [\![1..d]\!]\ \ i.a_i = 0 \iff \forall i \in [\![1..d]\!]\ \ a_i = 0$ ou $i \in p\mathbb{Z}$ (par déf de la caractéristique)
$\iff P(X) = \tilde{P}(X^p)$ où $\tilde{P} = \sum_{i=0}^{d/p} a_{ip} X^i$
$\iff P(X) = R(X)^p$ où $R = \sum_{i=0}^{d/p} b_i X^i$ où $b_i^p = a_{ip}$. ($b_i = a_{ip}^{p^{m-1}}$ où $q = p^m$ convient)
En effet un tel b_i existe par surjectivité du morphisme de Frobenius dans $\mathbb{K}$ fini et l'on a bien $R(X)^p = \left(\sum_{i=0}^{d/p} b_i X^i\right)^p = \sum_{i=0}^{d/p} (b_i X^i)^p = \sum_{i=0}^{d/p} b_i^p X^{ip} = \sum_{i=0}^{d/p} a_{ip} (X^p)^i = \tilde{P}(X^p)$

D'où l'algorithme : Réduction (P) :

```
Calculer P'
Si P' = 0  alors calculer réduction(R) où R^p = P
Si P' ≠ 0  calculer P1 = PGCD(P, P')
           Si P1 = 1  retourner P1
           Si P1 ≠ 1  calculer P2 = P/P1
                      calculer Réduction(P1)
                      ——— Réduction(P2)
```