123

Corps finis - Applications.

I. Caractéristique et sous-corps premier

Déf 1: Un corps est un anneau commutatif dans lequel tout élément non nul est inversible.

Déf 2: Un corps fini est un corps de cardinal fini.

rem 3: D'après le théorème de Wedderburn, tout corps gauche (non supposé commutatif) fini est commutatif.

Soit $\gamma : \begin{cases} \mathbb{Z} \longrightarrow \mathbb{K} \\ n \longmapsto \underbrace{1_{\mathbb{K}} + \dots + 1_{\mathbb{K}}}_{n} \end{cases}$ où $\mathbb{K}$ est un corps

γ est un morphisme d'anneaux donc son noyau est de la forme $\ker\gamma = p\mathbb{Z}$ pour $p \in \mathbb{N}$.

Déf 4: p est la caractéristique de $\mathbb{K}$, notée $\mathrm{car}(\mathbb{K})$.

Pté 5: $p = 0$ ou p est un nombre premier.

Pté 6: Soit $\mathbb{K}$ et $\mathbb{L}$ deux corps, tels que $\mathbb{K}$ est un sous-corps de $\mathbb{L}$, alors: $\mathbb{K}$ et $\mathbb{L}$ ont la même caractéristique.
- $\mathbb{L}$ peut être vu comme un $\mathbb{K}$-espace vectoriel
- Si $\mathbb{L}$ et $\mathbb{K}$ sont finis alors, il existe $n \in \mathbb{N}^*$ tel que $\mathrm{card}(\mathbb{L}) = \mathrm{card}(\mathbb{K})^n$

Sous-corps premier

Déf 7: Soit $\mathbb{K}$ un corps, son sous-corps premier est le corps engendré par $1_{\mathbb{K}}$.

pté 8: $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ n est premier

Pté 9: Soit $\mathbb{K}$ un corps et $\mathbb{P}$ son sous-corps premier. Alors,
Si $\mathrm{car}(\mathbb{K}) = 0$ alors $\mathbb{P} \cong \mathbb{Q}$
Si $\mathrm{car}(\mathbb{K}) = p < \infty$ alors $\mathbb{P} \cong \mathbb{Z}/p\mathbb{Z}$.

Cor 10: Si $\mathbb{K}$ est fini alors $\mathrm{car}(\mathbb{K}) \neq 0$ et il existe $n \in \mathbb{N}^*$ et p premier tel que $\mathrm{card}(\mathbb{K}) = p^n$

cor 11: Si $\mathbb{K}$ est de cardinal p, avec p un nombre premier, alors $\mathbb{K} \cong \mathbb{Z}/p\mathbb{Z}$

Rem 12: Pour p premier, il y a unicité à isomorphisme près du corps à p éléments!

Déf 13: On le note $\mathbb{F}_p$ $(\cong \mathbb{Z}/p\mathbb{Z})$

II. Comprendre la structure d'un corps fini

1) Endomorphisme de Frobenius et automorphismes

Soit $\mathbb{K}$ un corps de caractéristique p, de sous corps premier $\mathbb{P} \cong \mathbb{F}_p$.

Pté 14: $F^r : \begin{cases} \mathbb{K} \longrightarrow \mathbb{K} \\ x \longmapsto x^{p^r} \end{cases}$ est un homomorphisme.

Déf 15: On l'appelle morphisme de Frobenius.

Pté 16: $\forall r \in \mathbb{N}^*$, $\forall (a,b) \in \mathbb{K}$; $\forall (A,B) \in \mathbb{K}[X]$
$(a+b)^{p^r} = a^{p^r} + b^{p^r}$ et $(A+B)^{p^r} = A^{p^r} + B^{p^r}$

Pté 17:
- Si $\mathbb{K}$ est fini alors F^r est un isomorphisme
- Si $\mathrm{card}(\mathbb{K}) = p$ alors $F^r = \mathrm{id}_{\mathbb{K}}$

→ Les corps finis sont des corps parfaits

Pté 18: $\mathrm{Aut}(\mathbb{F}_p) = \{\mathrm{id}_{\mathbb{F}_p}\}$

Pté 19: $\forall x \in \mathbb{K}$, $x \in \mathbb{P} \Leftrightarrow x^p = x$
$\forall P \in \mathbb{K}[X]$, $P \in \mathbb{P}[X] \Leftrightarrow P(X^p) = P(X)^p$

Soit $\mathbb{K}$ fini de cardinal $q = p^n$ avec p premier et $n \in \mathbb{N}^*$.

Pté 20: $\forall P \in \mathbb{K}[X]$, $P(X^q) = P(X)^q$

Lemme 21: Pour $\alpha \in \mathbb{K}$ de degré r sur $\mathbb{P}$ de polynôme minimal μ_α sur $\mathbb{P}$ on a:
- r est le plus petit entier m tel que $\alpha^{p^m} = \alpha$
- les α^{p^i} pour $i \in \{0, \dots, r-1\}$ sont deux à deux différents
- $\mu_\alpha = \prod_{i=0}^{r-1} (X - \alpha^{p^i})$

Pté 22: $\mathrm{Aut}(\mathbb{K}) = \{F^{ri} \mid i \in \{0, \dots, n-1\}\} \cong \mathbb{Z}/n\mathbb{Z}$

Rem: Dans un corps fini, il existe des automorphismes non triviaux. (si $\mathrm{card}(\mathbb{K})$ n'est pas 1^n)

2) Sous-groupes de $\mathbb{K}^\times$

Pté 23 : Soit $\mathbb{K}$ un corps. Alors les sous-groupes finis de $\mathbb{K}^\times$ sont cycliques.

Rem 24 : En particulier, si $\mathbb{K}$ est un corps fini, alors $\mathbb{K}^\times$ est cyclique

Cor 25 : Théorème de l'élément primitif pour les corps finis.
Soit $\mathbb{L}$ une extension finie d'un corps fini $\mathbb{K}$. Alors, il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[\alpha]$.
On dit que α est l'élément primitif.

Rem 26 : Si α est un générateur de $\mathbb{L}^\times$ alors c'est un élément primitif de $\mathbb{L}$ sur $\mathbb{K}$.
Attention : La réciproque n'est pas vraie. Si on considère $\mathbb{K} = \mathbb{F}_2$ et $\mathbb{L} = \frac{\mathbb{F}_2[X]}{\Phi_5}$ où $\Phi_5 = X^4+X^3+X^2+X+1$

Alors, $\overline{X}$ est primitif mais n'engendre pas $\mathbb{L}^\times$ car $\overline{X}^5 = 1$.

3) Les carrés dans les corps finis

Soit $\mathbb{K}$ un corps à $q = p^n$ éléments.
On pose $\mathbb{K}^\square = \{a^2 \mid a \in \mathbb{K}\}$ et $\mathbb{K}^{\square\times} = \mathbb{K}^\square \cap \mathbb{K}^\times$

Pté 27 :
- Si $p=2$ alors $\mathbb{K}^\square = \mathbb{K}$
- Si $p>2$ alors :
  - $\mathbb{K}^{\square\times}$ est un sous-groupe d'indice 2 de $\mathbb{K}^\times$
  - $\mathbb{K}^{\square\times}$ est de cardinal $(q-1)/2$
  - $\mathbb{K}^{\square\times}$ est le noyau du morphisme $x \mapsto x^{\frac{q-1}{2}}$ de $\mathbb{K}^\times$
  - $(-1) \in \mathbb{K}^{\square\times} \iff q \equiv 1 [4]$

Cor 28 : Il existe une infinité de nombre premier de la forme $4k+1$

a. Calcul des carrés dans $\mathbb{F}_p$, p premier

Déf 29 : Pour $x \in \mathbb{F}_p^\times$, le symbole de Legendre $\left(\frac{x}{p}\right)$ est défini par $\left(\frac{x}{p}\right) = 1 \iff x \in \mathbb{F}_p^{\square\times}$ et $\left(\frac{x}{p}\right) = -1$ sinon.

Pté 30 : (Euler), $\forall x \in \mathbb{F}_p^\times$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$

Pté 31 : Pour p premier et $x, y \in \mathbb{F}_p^\times$ on a :
- $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$
- $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 [4]$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Théorème 32 : (Loi de réciprocité quadratique) pour p et ℓ premiers impairs
$$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}$$

Ex 33 : $\left(\frac{45}{79}\right) = \left(\frac{3}{79}\right)^2\left(\frac{5}{79}\right) = \left(\frac{79}{5}\right) = \left(\frac{-1}{5}\right) = 1$ donc 45 est un carré dans $\mathbb{F}_{79}$

Déf 34 : Si $N = \prod p_i^{\alpha_i}$ n'est pas premier, on définit le symbole de Jacobi $\left(\frac{x}{N}\right) = \prod \left(\frac{x}{p_i}\right)^{\alpha_i}$

Pté 35 : le symbole de Jacobi respecte la propriété 31 et le Thm 32 en remplaçant p par N.

Rem 36 : $\left(\frac{x}{N}\right) = 1$ ne veut pas dire que x est un carré modulo N.
Le symbole de Jacobi permet de calculer les symboles de Legendre beaucoup plus efficacement en évitant la factorisation en facteurs premiers.

Carrés dans un corps de cardinal $q = p^n$

$\mathbb{K}$ de cardinal q et $\mathbb{F}_p$ sous-corps premier.

Déf 37 : Pour $a \in \mathbb{K}$, sa norme $N(a)$ est le déterminant de l'application $\mathbb{F}_p$-linéaire : $x \mapsto ax$ de $\mathbb{K}$.

Pté 38 : a est un carré dans $\mathbb{K} \iff N(a)$ est un carré dans $\mathbb{F}_p$.

III. Les corps finis : existence, unicité et inclusions

1) Construction théorique par les corps de décomposition

Pté 38 : Soit $\mathbb{K}$ un corps à $q = p^m$ éléments. ($\mathbb{F}_p$ est son sous-corps premier).
Alors $\mathbb{K}$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Pté 39 : Il y a unicité du corps de décomposition à isomorphisme près.

Cor 40 : Deux corps finis de même cardinal sont isomorphes.

Rem 41 : la (pté 22) montre que l'isomorphisme entre deux corps finis de même cardinal n'est pas unique.

pté 42 : le corps de décomposition du polynôme $X^{p^r} - X$ sur $\mathbb{F}_p$ a p^r éléments, ceci $\forall r \in \mathbb{N}^*$.

Rem 43 : On a établit que pour tout p premier et r entier, il existe un unique corps à p^r éléments à isomorphisme près.

Déf 44 : On note le corps à $p^r = q$ éléments $\mathbb{F}_q$.

2) Construction pratique de $\mathbb{F}_q$ grâce aux corps de rupture

Ptié 45 : Soit Q un polynome irréductible sur $\mathbb{F}_p$ de dégré r. Alors $\mathbb{F}_p[X]/(Q)$ est un corps de cardinal q^r.

Rem 46 : Soit Q un polynome irreductible sur $\mathbb{F}_p$ et α une racine de Q dans $\mathbb{F}_p(X)/(Q)$, (par exemple $\alpha = \bar{X}$) alors $\mathbb{F}_p[X]/(Q) \cong \mathbb{F}_p[\alpha]$.

Ex 47 : Construction de $\mathbb{F}_{4} \cong \mathbb{F}_2[X]/Q$ où $Q = X^2+X+1$ irreductible. α racine de Q. Les éléments de $\mathbb{F}_4$ sont $0, 1, \alpha$ et $\alpha^2 = \alpha+1$. On obtient facilement la table de multiplication (Annexe)

3) Sous-corps de $\mathbb{F}_{p^n}$

Lemme : $a, b \in \mathbb{N}$, p premier. alors $p^a-1 \mid p^b-1 \iff a \mid b$

Ptié 48 : Les sous-corps de $\mathbb{F}_{p^n}$ sont exactement les $\mathbb{F}_{p^d}$ pour $d \mid n$.

Rem 49 : $\mathbb{F}_{p^n}$ peut alors être vu comme un $\mathbb{F}_{p^d}$-EV de dim (n/d).

Ex 50 : Sous-corps de $\mathbb{F}_{2^{20}}$ (Annexe)

IV. Polynômes sur les corps finis.

1) Cloture algébrique.

Ptié 51 : Un corps fini n'est jamais algébriquement clot.
↳ considérer le polynôme $\prod_{\alpha \in \mathbb{K}} (X-\alpha) + 1$. ($\mathbb{K}$ est le corps fini)

Ptié 52 : $\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$ est la cloture algébrique de tout corps fini de caracteristique p.

2) Polynômes cyclotomiques sur un corps fini.

- Les polynômes cyclotomiques ϕ_n sont à coefficients dans $\mathbb{Z}$ (même dans $\{-1, 0, 1\}$ donc on peut les regarder comme polynôme de $\mathbb{F}_q[X]$.

Rem 53 : Les polynômes cyclotomiques sont irréductibles dans $\mathbb{Z}[X]$, mais ne le sont pas forcément dans $\mathbb{F}_q[X]$:
Dans $\mathbb{F}_2[X]$, ϕ_7 s'écrit : $\phi_7 = (1+X+X^3)(1+X^2+X^3)$.

Ptié 54 : Soit $q = p^n$ et m premier avec q. Notons r l'ordre de q dans $(\mathbb{Z}/m\mathbb{Z})^\times$. Alors, ϕ_m se décompose dans $\mathbb{F}_q[X]$ comme produit de polynômes irréductibles de degré r tous différents.

Ex 55 : $q=2$, $m=7$; $2 \neq 1 [7]$, $2^2 \neq 1 [7]$ mais $2^3 \equiv 1 [7]$. $r=3$

Cor 56 : ϕ_m est irréductible dans $\mathbb{F}_q[X]$ si et seulement si $\langle q \rangle = (\mathbb{Z}/n\mathbb{Z})^\times$.

Ex 57 : Pour tout $q = p^n$, $\phi_8 = X^4+1$ n'est pas irréductible sur $\mathbb{F}_q[X]$.

Cor 58 : Dans $\mathbb{F}_p[X]$, ϕ_{p^r-1} s'écrit comme produit de polynômes irréductibles de degré r.

Rem 59 : Ceci assure l'existence de polynômes irréductible de tout degré sur $\mathbb{F}_p[X]$ donc par passage au corps de rupture l'existence d'un corps de cardinal p^r, $\forall p$ premier, $\forall r \in \mathbb{N}$

3) Polynomes irréductibles dans $\mathbb{F}_q[X]$

Soit $q = p^n$

Ptié 60 : Dans $\mathbb{F}_q[X]$, $X^{q^r} - X$ est le produit des polynomes irréductibles dont le degré divise r.
→ La propriété suivante permet de déterminer de façon pratique si un polynome est irréductible.

Ptié 61 : P irréductible dans $\mathbb{F}_q[X]$ de degré r si et seulement si :
- $P \mid X^{q^r} - X$ et pour tout facteur premier de r on ait
- $P \wedge (X^{q^{r/\ell}} - X) = 1$.

Ptié 62 : le nombre de polynomes irréductible de degré r sur $\mathbb{F}_q[X]$ est égal à $\sum \mu(\frac{r}{d}) q^d$ où μ est la fonction de Möbius.

Ex 63 : Dans $\mathbb{F}_3[X]$, il y a $\frac{1}{6}(3^6 - 3^3 - 3^2 + 3^1) = 116$ polynômes de degré 6 dont 696 irréductibles.

4) Algorithmes de factorisation : But : Trouver les facteurs irréductibles d'un polynôme P dans $\mathbb{F}_q[X]$

Algorithme de Berlekamp

- On se ramène à P sans facteurs multiples
- On calcule la matrice de $\alpha \mapsto \alpha^p =: S$ dans le $\mathbb{F}_p$-EV $\mathbb{F}_p[X]/(P)$
- On détermine $\ker(S-I)$.
- Si $\dim(\ker(S-I)) = 1$ alors P est irréductible.
  Sinon Pour chaque $\alpha \in \mathbb{F}_q$ calculer $d_\alpha = \mathrm{PGCD}(P, Q-\alpha)$
  . Si $d_\alpha \neq 1$ alors appliquer l'algo à d_α.

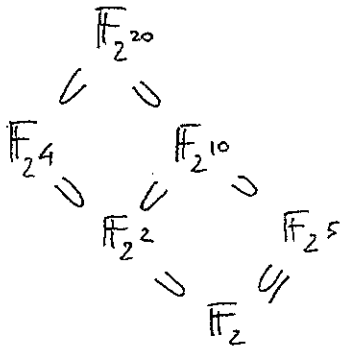
Algorithme de Cantor-Zassenhaus

- On se ramène à $P = P_1 \cdots P_s$ avec $P_i \neq P_j$ $\forall i,j$ et $\deg P_1 = \cdots = \deg P_s = r$
- On choisit Q de degré $\leq 2r$ dans $\mathbb{F}_q[X]$
- On calcule $\mathrm{PGCD}(P, Q)$; $\mathrm{PGCD}(P, Q^{\frac{r-1}{2}} - 1)$ et $\mathrm{PGCD}(P, Q^{\frac{r-1}{2}} + 1)$ avec proba $\geq 1/2$, cette factorisation est non triviale et on réapplique l'algo aux morceaux obtenus.
  Sinon On recommence avec un autre $Q \in \mathbb{F}_q[X]$. Proba d'échec : $\leq 2^{-m}$
- On s'arrête après m coup.

Table de multiplication de $\mathbb{F}_4 \cong \mathbb{F}_2[\alpha]$.

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Sous-corps de $\mathbb{F}_{2^{20}}$:



Bibliographie :

- Daniel Perrin, Cours d'Algèbre. Ellipses
- I. Gozard, Théorie de Galois, Ellipses.
- J. Calais, Extensions de corps, Ellipses
- M. Demazure. Cours d'Algèbre. Cassini
- D. Hernandez, Y. Laszlo. Introduction à la théorie de Galois, éd de l'X.

Se ramener à un polynôme sans facteur multiple.

Objectif Agrégation 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 caractéristique $\neq 0$).
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 $P' = \sum_{j=1}^{s} \left(\prod_{\substack{i=1 \\ i\neq j}}^{s} P_i^{\alpha_i} \right) \times \alpha_j P_j' P_j^{\alpha_j - 1}$

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

$\forall j \in [\![1..s]\!]$ $P_j \mid Q$ 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 $\alpha_j \cdot 1_{\mathbb{K}} = 0$
À en tant que diviseur de P on sait que le $PGCD(P, P')$ s'écrit comme produit de certain des P_i, on sait 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 $\alpha_i \cdot 1_{\mathbb{K}} \neq 0$ évidemment)
ou $\alpha_i > 0$

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 :

Pté Si $\mathbb{K}$ est un corps fini de caractéristique p et si $P \in \mathbb{K}[X]$
alors $PGCD(P,P') = P \Leftrightarrow P' = 0$
$\Leftrightarrow \exists \tilde{P} \in \mathbb{K}[X],\ P(X) = \tilde{P}(X^p)$
$\Leftrightarrow \exists R \in \mathbb{K}[X]\ P(X) = R(X)^p$
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 $\deg(P) \leq \deg(P')$.
A sauf pour $P = 0$ (qui implique $P' = 0$) $\deg(P') < \deg(P)$.
On a donc ici $P' = 0$. La réciproque est claire car P est le plus grand diviseur de P et il divise aussi 0.

• On écrit $P = \sum_{i=0}^{d} a_i X^i$ $\quad P' = \sum_{i=1}^{d} i.a_i X^{i-1}$
$P' = 0 \Leftrightarrow \forall i \in [\![1..d]\!]\ i.a_i = 0 \Leftrightarrow \forall i \in [\![1..d]\!]\ a_i = 0$ ou $i \in p\mathbb{Z}$ (par déf de la caractéristique)
$\Leftrightarrow P(X) = \tilde{P}(X^p)$ où $\tilde{P} = \sum_{i=0}^{d/p} a_{ip} X^i$
$\Leftrightarrow P(X) = R(X)^p$ où $R = \sum_{i=0}^{d/p} b_i X^i$ où $b_i^p = a_{ip}$. ($b_i = a_{ip}^{p^{m-1}}$ convient où $q = p^m$)
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)
```

Réduction d'un produit de facteurs irréductibles de même degré

Cf Demazure p234 "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 irréductibles 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 Cantor-Zassenhaus fonctionne. Cf 93.

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 irréductibles unitaires dont le degré divise n.

Preuve Soit $P \in \mathbb{F}_q[X]$ un polynôme irréductible 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 Lagrange).
En itérant k fois on 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 $F^n - \mathrm{id}_{\mathbb{K}}$ 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 $A = \mathbb{K}$.
$\mathbb{K}^\times$ 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) :
$P = \prod_{i=1}^{n} P_i$. On a alors $P = \prod_{j=1}^{m} R_j$ où $R_j = \prod_{\substack{i=1 \\ \deg P_i = j}}^{n} P_i$ 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 $\cdot \forall j \in [1..n]$ $\mathrm{PGCD}(P, X^{q^j} - X) = \prod_{\substack{k=1 \\ k \mid j}}^{n} R_k$ (1)

$\cdot \forall j \in [1..n]$ $R_j = \left(\dfrac{\mathrm{PGCD}(P, X^{q^j} - X)}{\prod_{\substack{k \mid j \\ k \neq j}} R_k} \right)$ (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 $\mathrm{PGCD}(P, X^{q^j} - X) = \prod_{\deg(P_i) \mid j} P_i$ ce qui en réorganisant les facteurs par mêmes degrés $\mathrm{PGCD}(P, X^{q^j} - X) = \prod_{k \mid j} \prod_{\deg(P_i) = k} P_i = \prod_{k \mid j} R_k$.
D'où (1).
Cela donne aussi $\mathrm{PGCD}(P, X^{q^j} - X) = \prod_{\substack{k \mid j \\ k \neq j}} R_k \times R_j$ d'où (2).

On en déduit l'algorithme suivant

Réduction_en_degré(P) :

```
m = deg(P) . i = 1
tant que i ≤ m
    calculer Q = PGCD(P, X^(q^i) - X)
    si i premier alors stocker R_i = Q
    sinon stocker R_i = Q / (produit des R_j pour j | i, j ≠ i)
    faire m := m / deg(R_i)
```

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

Algorithme de Berlekamp

Cf Object Agrégation p245.
Demazure, cours d'algèbre p232.

Le but de cet algorithme est de fournir la décomposition en produit de facteurs irréductibles d'un polynôme sur un corps fini. On se restreint à des polynômes sans facteurs multiples, sachant s'y ramener d'après 96.

Soit p un nombre premier. Soit $n \in \mathbb{N}^*$. On pose $q = p^n$
Soit $P \in \mathbb{F}_q[X]$, un polynôme sans facteur multiple.
La décomposition en facteurs irréductibles (DFI) s'écrit alors $P = \prod_{i=1}^{s} P_i$. Notons $d = \deg(P)$.

Notons que P est irréductible ssi $s = 1$.

98.1 **Berlekamp (P) :**

- Pour j allant de 0 à $d-1$ calculer $(X^j)^q$ modulo (P).
- En déduire $M = Mat_{\mathcal{B}}(S)$ où $\mathcal{B} = (1, X, \dots X^{d-1})$ base de $\mathbb{F}_q[X]/(P)$
  $S = \left(\begin{smallmatrix} \mathbb{F}_q[X] \to \mathbb{F}_q[X] \\ \alpha \mapsto \alpha^q \end{smallmatrix}\right)$
- Par le pivot de Gauss calculer $\ker(M - Id) = K$
- Si $\dim K = 1$
  alors renvoyer P
  sinon choisir $V \in K$ non constant
  : pour chaque $\alpha \in \mathbb{F}_q$, calculer $d_\alpha = PGCD(P, V - \alpha)$
  et appliquer Berlekamp à d_α (si $d_\alpha \neq 1$)

98.2 **Ptés** Cet algorithme termine nécessairement et fournit bien une DFI de P.

Preuve : 1) LEMME CHINOIS ET ISOMORPHISME

(On note $A \wedge B$ pour $PGCD(A, B)$)

On a $\forall (i,j) \in [\![1..s]\!]^2 \ i \neq j \Rightarrow (P_i, P_j) = (P_i \wedge P_j) = (1) = \mathbb{F}_q[X]$
De plus $\bigwedge_{i=1}^{s} (P_i) = \left(\prod_{i=1}^{s} P_i\right) = (P)$.

On peut donc appliquer le lemme chinois qui assure que :

$\gamma = \left(\begin{array}{ccc} A := \mathbb{F}_q[X]/(P) & \longrightarrow & \prod_{i=1}^{s} A_i := \mathbb{F}_q[X]/(P_i) \\ \overline{Q}^{(P)} & \longrightarrow & \left(\overline{Q}^{(P_i)}\right)_{i \in [\![1..s]\!]} \end{array} \right)$ est un isomorphisme d'anneau.

(où $\overline{Q}^{(P)}$ désigne la classe de Q modulo P ie $\{Q + RP \mid R \in \mathbb{F}_q[X]\}$
$\overline{Q}^{(P_i)}$ ——— P_i ie $\{Q + RP_i \mid$ ——— $\}$)

En fait γ est même un isomorphisme de $\mathbb{F}_q$-EV.

En effet si $\lambda \in \mathbb{F}_q[X]$ et $\overline{Q} \in A$

$\lambda . \gamma(\overline{Q}^{(P)}) = \lambda . \left(\overline{Q}^{(P_i)}\right)_{i \in [\![1..s]\!]}$

$= \left(\lambda . \overline{Q}^{(P_i)}\right)_{i \in [\![1..s]\!]}$) déf d'EV produit.

$= \left(\overline{\lambda \times_{\mathbb{F}_q[X]} Q}^{(P_i)}\right)$) déf de la structure de $\mathbb{F}_q$-EV de A_i vu comme quotient d'EV

$= \gamma\left(\overline{\lambda \times_{\mathbb{F}_q[X]} Q}^{(P)}\right)$

$= \gamma(\lambda . \overline{Q}^{(P)})$) déf de la structure de $\mathbb{F}_q$-EV de A vu comme quotient d'EV.

2) CALCUL DE s

On introduit $S = \left(\begin{array}{ccc} A & \to & A \\ \overline{Q}^{(P)} & \mapsto & \overline{Q^q}^{(P)} \end{array} \right)$ et pour $i \in [\![1..s]\!]$ $S_i = \left(\begin{array}{ccc} A_i & \to & A_i \\ \overline{Q}^{(P_i)} & \mapsto & \overline{Q^q}^{(P_i)} \end{array} \right)$

Ce sont les puissances n-ièmes resp. des morphismes de Frobenius.

On note $A^S = \{x \in A \mid S(x) = x\} = \ker(S - id_A)$ les points fixes de S.

Soit $\overline{Q}^{(P)} \in A$.

$\overline{Q}^{(P)} \in A^S \Leftrightarrow S(\overline{Q}^{(P)}) = \overline{Q}^{(P)}$

$\Leftrightarrow \gamma(\overline{Q^q}^{(P)}) = \gamma(\overline{Q}^{(P)})$) car γ bijective

$\Leftrightarrow \forall i \in [\![1..s]\!] \quad \overline{Q^q}^{(P_i)} = \overline{Q}^{(P_i)}$

$\Leftrightarrow \forall i \in [\![1..s]\!] \quad \overline{Q}^{(P_i)^q} = \overline{Q}^{(P_i)}$) Lemme : Si $\mathbb{K}$ est une ext de $\mathbb{F}_q$ alors $\forall x \in \mathbb{K}$, $x \in \mathbb{F}_q$ ssi $x^q = x$

$\Leftrightarrow \forall i \in [\![1..s]\!] \quad \overline{Q}^{(P_i)} \in \underbrace{\mathbb{F}_q . 1_{A_i}}$ droite vectorielle de A_i

$\Leftrightarrow \gamma(\overline{Q}^{(P)}) \in \bigoplus_{i=1}^{s} \mathbb{F}_q . 1_{A_i}$

Donc $\dim_{\mathbb{F}_q}(A^S) = \dim\left(\bigoplus_{i=1}^{s} \mathbb{F}_q . 1_{A_i}\right) = s$ soit $\underline{\underline{s = \dim_{\mathbb{F}_q}(A^S)}}$

(car γ iso de $\mathbb{K}$-EV)

Alors que ce qui se passe du côté des A_i se fait "en boîte noire", on a accès aux points fixes de S du côté de A : c'est le $\underbrace{\ker(M - I_d)}_{K}$ qu'on a calculé d'où $\underline{s = \dim(K)}$

3) COMPRENDRE LES PGCD $(P, V-\alpha)$

Dans le cas où s valait 1 on s'est arrêté car cela signifiait P irréductible.
Supposons maintenant $s \geq 1$. A^S étant de dimension > 1 il ne peut être réduit à $\mathbb{F}_q.1_A$ qui est la droite vectorielle des classes de polynômes constants modulo (P). Il existe donc $\overline{Q}^{(P)} \in A^S \setminus \mathbb{F}_q.1_A$.
$\forall i \in [1..s]$ $\overline{Q}^{(P_i)} \in \mathbb{F}_q.1_{A_i}$ d'après l'équivalence précédente.

Rq Dans les A_i les points fixes de S_i sont les classes de polynômes constants justement parce que les P_i sont irréductibles.

Choisissons de meilleurs représentants :

MQ $\forall \alpha \in \mathbb{F}_q$, $\mathrm{PGCD}(P, Q-\alpha) = \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{S} P_i$

Soit $i \in [1..s]$ $\overline{Q}^{(A_i)} = \overline{\alpha_i X^0}^{(A_i)}$ soit $Q - \alpha_i \equiv 0 [P_i]$ soit $P_i \mid Q - \alpha_i$

↳ si $\alpha = \alpha_i$ $P_i \mid Q - \alpha$

↳ si $\alpha \neq \alpha_i$ $Q - \alpha \equiv Q - \alpha_i + \alpha_i - \alpha \equiv \alpha_i - \alpha \ [P_i]$ or α_i et α étant des constantes leur différence n'est pas résidue modulo (P_i), autrement dit $\alpha_i - \alpha \not\equiv 0 [P_i]$
donc $P_i \nmid Q - \alpha_i$

Comme $\mathrm{PGCD}(P, Q-\alpha)$ s'écrit, en tant que diviseur de P, naturellement comme produit de certains P_i on en déduit $\mathrm{PGCD}(P, Q-\alpha) = \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{S} P_i$.

On en déduit que $P = \prod_{i=1}^{S} P_i = \prod_{\alpha \in \mathbb{F}_q} \prod_{\substack{i=1 \\ \alpha_i = \alpha}}^{S} P_i = \prod_{\alpha \in \mathbb{F}_q} \mathrm{PGCD}(P, Q-\alpha)$

Et cette décomposition est meilleure car calculable. Il reste cependant à montrer qu'elle n'est pas triviale, c-à-d qu'il n'existe aucun terme valant P.
$\mathrm{PGCD}(P, Q-\alpha) = P$ ssi $\forall i \in [1..s]$ $\alpha_i = \alpha$ ssi $(\overline{Q}^{(P_i)})_{i \in [1..s]} = (\overline{\alpha X^0}^{(P_i)})_{i \in [1..s]}$
ssi $\gamma(\overline{Q}^{(P)}) = \gamma(\overline{\alpha X^0}^{(P)}) = \gamma(\alpha . 1_A)$ ssi $\overline{Q}^{(P)} = \alpha . 1_A$
IMPOSSIBLE car on a pris $\overline{Q}^{(P)}$ "non constant" c-à-d n'appartenant pas à $\mathbb{F}_q.1_A$.
Ceci assure que cette décomposition fournit au moins deux facteurs stricts de P, de degré strictement moindre. Ainsi l'algorithme termine nécessairement.

Algorithme de Cantor-Zassenhaus. Q Demazure Cours d'Algèbre p 234.

Comme l'algorithme de Berlekamp, Cantor-Zassenhaus a pour but de fournir la décomposition en facteur irréductible (DFI) d'un polynôme sur un corps fini. Attention on se restreint ici aux polynômes sans facteurs multiple et dont tous les facteurs sont de même degré, sachant qu'on peut s'y ramener algorithmiquement d'après 96 et 97.

Soit p un nombre premier ≥ 2. Soit $n \in \mathbb{N}^*$. On pose $q = p^n$.
Soit $P \in \mathbb{F}_q[X]$ un polynôme sans facteurs multiple et dont tous les facteurs irréductibles sont de degré r, supposé connu (Cf 97).
La DFI de P s'écrit alors $P = \prod_{i=1}^{s} P_i$ où $\forall i \in [\![1,s]\!]$ $\deg(P_i) = r$.

Ptié $\forall Q \in \mathbb{F}_q[X]$ $\quad P = PGCD(P, Q^{q^r} - Q) \times PGCD(P, Q^{\frac{q^r-1}{2}} - 1) \times PGCD(P, Q^{\frac{q^r-1}{2}} + 1)$

Preuve 1) MONTRER QUE $P \mid Q^{q^r} - Q$

- Puisque $X^{q^r} - X$ est le produit de tous les irréductibles de $\mathbb{F}_q$ de degré divisant r (Cf 93) il est en particulier divisible par P. Donc $P \mid X^{q^r} - X$
- Montrons que $X^{q^r} - X \mid Q^{q^r} - Q$. Si $Q = \sum_{i=1}^{d} a_i X^i$

$$Q^{q^r} = \Big(\sum_{i=1}^{d} a_i X^i\Big)^{q^r} \underset{\text{Frobenius fois prolongé aux polynômes}}{=} \sum_{i=1}^{d} (a_i X^i)^{q^r} = \sum_{i=1}^{d} \underbrace{(a_i)^{q^r}}_{a_i \text{ car } a_i \in \mathbb{F}_q} X^{i \times q^r} = \sum_{i=1}^{d} a_i X^{i \times q^r}$$

Donc $Q^{q^r} - Q = \sum_{i=1}^{d} a_i \left((X^{q^r})^i - X^i\right)$ or $\forall i \in [\![1,d]\!]$ $X^{q^r} - X \mid (X^{q^r})^i - X^i$
donc $X^{q^r} - X \mid Q^{q^r} - Q$. (utiliser la formule $(a^n - b^n) = (a-b)\left(\sum_{i=0}^{n-1} a^i b^{n-1-i}\right)$)
- Par transitivité $P \mid Q^{q^r} - Q$

2) CONCLURE

$$\cdot\ Q^{q^r} - Q = Q(Q^{q^r-1} - 1) = Q\left((Q^{\frac{q^r-1}{2}})^2 - 1^2\right) = Q\underbrace{\left(Q^{\frac{q^r-1}{2}} + 1\right)}_{:=Q_1}\underbrace{\left(Q^{\frac{q^r-1}{2}} - 1\right)}_{:=Q_2}.$$

- $\frac{1}{2}Q_1 - \frac{1}{2}Q_2 = 1$ donc $PGCD(Q_1, Q_2) = 1$
- $-Q^{\frac{q^r-1}{2}-1} \times Q + 1 \times Q_1 = 1$ donc $PGCD(Q, Q_1) = 1$
- $Q^{\frac{q^r-1}{2}-1} \times Q - 1 \times Q_2 = 1$ donc $PGCD(Q, Q_2) = 1$

$\Big\}$ $PGCD(P, Q \times Q_1 \times Q_2) = PGCD(P,Q) \times PGCD(P,Q_1) \times PGCD(P,Q_2)$

Or $PGCD(P, Q \times Q_1 \times Q_2) = PGCD(P, Q^{q^r} - Q)$
$= P$ car $P \mid Q^{q^r} - Q$.

□

Pté Si P est non irréductible et si Q est choisi aléatoirement parmi les polynômes de $\mathbb{F}_q[X]$ de degré $\leq 2r$, la probabilité que la décomposition $P = PGCD(P,Q) \times PGCD(P,Q_1) \times PGCD(P,Q_2)$ soit triviale est inférieure à $\frac{2}{2^s}$ où ~~$s = \log_r(\deg(P))$~~ $s = \frac{\deg P}{r}$

Preuve Puisque P non irréductible $s \geq 2$.

Pour $(i,j) \in [\![1..q]\!]^2$ tel que $i \neq j$ on considère $\begin{cases} \mathbb{K}_i = \mathbb{F}_q(X)/(P_i) \\ \mathbb{K}_j = \mathbb{F}_q(X)/(P_j) \end{cases}$

Puisque $\deg(P_i) = \deg(P_j) = r$ on a $\#\mathbb{K}_i = \#\mathbb{K}_j = q^r$.

On pose $\varphi_{i,j} = \left(\begin{array}{ccc} \mathbb{F}_q[X]_{<2r} & \longrightarrow & \mathbb{K}_1 \times \mathbb{K}_2 \\ Q & \longmapsto & (\overline{Q}^{(P_1)}, \overline{Q}^{(P_2)}) \end{array} \right)$ où $\overline{Q}^{(P_1)}$ = classe de Q modulo (P_1)

$\overline{Q}^{(P_2)}$ = ——— (P_2).

$\varphi_{i,j}$ est un morphisme d'anneau.

MQ $\varphi_{i,j}$ INJECTIVE

$\forall Q \in \mathbb{F}_q[X]_{<2r}$ $Q \in \ker \varphi_{ij} \Leftrightarrow \varphi(Q) = (0,0) \Leftrightarrow P_1 | Q$ et $P_2 | Q$

$\Rightarrow P_1 P_2 | Q$ (car $P_1 \wedge P_2 = 1$)

$\Rightarrow Q = 0$ ou $\deg(Q) \geq \deg(P_1 P_2) = 2r$

$\Rightarrow Q = 0$ car $\deg(Q) < 2r$

Donc φ est injective (Et par suite bijective car $\#\mathbb{F}[X]_{<2r} = \#\mathbb{F}[0..q^{2r}-1] = q^{2r} = q^{2r} = \#\mathbb{K}_1 \times \#\mathbb{K}_2$)

Soit $Q \in \mathbb{F}_q[X]_{<2r}$ unitaire. → MQ LE PRODUIT EST TRIVIAL $\Rightarrow \overline{Q}^{(P_1)}$ et $\overline{Q}^{(P_2)}$ SONT DE LA NATURE QUADRATIQUE

Le produit est dit trivial si l'un des termes vaut P (et alors les autres 1).

- $PGCD(Q,P) = P \Leftrightarrow P|Q \Rightarrow \begin{matrix} P_i | Q \\ P_j | Q \end{matrix} \Rightarrow \begin{matrix} \overline{Q}^{(P_i)} = 0 \\ \overline{Q}^{(P_j)} = 0 \end{matrix} \Rightarrow \varphi_{i,j}(Q) = 0 \Rightarrow Q = 0$ IMP car Q unitaire.

- $PGCD(Q_1,P) = P \Leftrightarrow P|Q_1 \Rightarrow \begin{matrix} P_i | Q_1 \\ P_j | Q_1 \end{matrix} \Rightarrow \begin{cases} \overline{Q^{\frac{r-1}{2}}}^{(P_i)} = 1 = 1_{\mathbb{K}_i} \\ \overline{Q^{\frac{r-1}{2}}}^{(P_j)} = 1 = 1_{\mathbb{K}_j} \end{cases}$

$\Rightarrow \begin{cases} q_i^{\frac{r-1}{2}} = 1 \\ q_j^{\frac{r-1}{2}} = 1 \end{cases}$ où $q_i = \overline{Q}^{(P_i)}$ et $q_j = \overline{Q}^{(P_j)}$.

$\Rightarrow q_i$ et q_j sont résidus quadratiques.

- De même $PGCD(Q,P) = P \Rightarrow \begin{cases} q_i^{\frac{q^r-1}{2}} = -1 \\ q_j^{\frac{q^r-1}{2}} = -1 \end{cases} \Rightarrow q_i$ et q_j ne sont pas résidus quadratiques

RÉSUMER

On note $(q_i)_{i \in [\![1..s]\!]}$ les $\left(\overline{Q}^{(P_i)}\right)_{i \in [\![1..s]\!]}$

Si le produit est trivial soit tous les q_i sont des résidus quadratiques, soit tous les q_i ne sont pas résidus quadratiques.

MAJORER LA PROBABILITÉ

On admet que si on choisit Q uniformément parmi les polynômes unitaires de $\mathbb{F}_q[X]$ de degré $< 2r$, les $(q_i)_{i \in [\![1..s]\!]}$ suivent chacune une loi uniforme sur $\mathbb{F}_q[X]/(P_i)^\times = \mathbb{K}_i^\times$. Or puisque $\mathbb{K}_i^{\times\square}$ est un sous groupe d'indice 2 de $\mathbb{K}_i^\times$, cela implique l'on a une chance sur deux que q_i soit dans $\mathbb{K}_i^{\times\square}$, une chance sur deux qu'il ne soit pas résidu quadratique. On en déduit (indépendance des q_i) que la probabilité que tous les q_i soient des carrés est $1/2^s$ et celle qu'ils soient tous non résidus quadratique est aussi $1/2^s$. La probabilité que le produit soit trivial est donc majorée par $1/2^s + 1/2^s = 2/2^s$

Notant que les facteurs $\mathrm{PGCD}(P,Q)$, $\mathrm{PGCD}(P,Q_1)$ et $\mathrm{PGCD}(P,Q_2)$ sont encore sans facteur multiples et produit d'irréductibles de même degré r (tout ça parce qu'ils divisent P) on a l'algorithme probabiliste suivant.

Cantor-Zassenhaus (P, r, ε) : où P produit d'irréductibles 2à2 ≠ de même degré r, ε un paramètre fixant la précision de l'algo.

$n = \deg(P)$
s tel que $s = \frac{n}{r}$
k le plus petit tel que $(2^{1-s})^k \leq \varepsilon$

On choisit Q aléatoirement parmi les polynômes unitaires de $\mathbb{F}_q[X]$ de degré $< 2r$.
On calcule $Q_1 = Q^{q\frac{r-1}{2}} - 1 \mod P$
$Q_2 = Q^{q\frac{r-1}{2}} + 1 \mod P$
$A_0 = \mathrm{PGCD}(P,Q)$
$A_1 = \mathrm{PGCD}(P,Q_1)$
$A_2 = \mathrm{PGCD}(P,Q_2)$

Si $A_1 \neq P$ et $A_2 \neq P$ on appelle récursivement l'algo sur A_0, A_1, A_2, sachant que la factorisation de P sera le produit de celles de A_0, A_1 et A_2,
Sinon on choisit un nouveau Q aléatoirement et on recommence.
Toutefois si après k étapes on n'a eu que des produits triviaux, on renvoit P considérant qu'il est irréductible, sachant que le risque que ce soit à tort est $\leq \varepsilon$.