Année 2020-2021
L3 Mathématiques-Informatique

Université de Bordeaux
Stage

Factorisation de polynômes à coefficients dans un corps fini

Ronan Thoraval

30 juin 2021

Résumé

L'anneau des polynômes à coefficients dans un corps fini est un anneau euclidien, c'est-à-dire qu'il existe une division euclidienne d'un polynôme P par n'importe quel autre polynôme non-nul S dans cet anneau. On la définit comme suit :

$$P(X) = Q(X) \cdot S(X) + R(X)$$

où $R(X)$ est un polynôme de degré strictement inférieur à celui de $Q(X)$. Cette division est unique, à un inversible près, tout comme la décomposition d'un polynôme en produit de puissances de polynômes irréductibles, qui sont des polynômes non-inversibles et non-factorisables non-trivialement.

Plus formellement, un polynôme P à coefficients dans un corps fini $\mathbb{K}$ est irréductible si et seulement si

$$P(X) \notin \mathbb{K}^\times \text{ et } P(X) = Q(X) \cdot S(X) \implies \begin{cases} Q(X) \in \mathbb{K}^\times \\ ou \\ S(X) \in \mathbb{K}^\times \end{cases}$$

On peut faire un parallèle avec les nombres premiers de $\mathbb{Z}$, et, tout comme dans $\mathbb{Z}$, expliciter cette factorisation est un problème concret qui se pose.

Nous allons donc voir dans ce mémoire comment factoriser ces polynômes, et par conséquent, comment reconnaitre un irréductible.

Bonne lecture !

Table des matières

1 Quelques propriétés des corps commutatifs

Définition 1 :

Un ***corps*** *est un anneau non-nul dans lequel tous les éléments non-nuls sont inversibles :*
Si $\mathbb{A}$ *est un anneau alors*

$$\mathbb{A} \text{ est un corps } \Leftrightarrow \mathbb{A}^\times = \mathbb{A}^*$$

Définition 2 :

Un corps ***commutatif*** *est un corps* $\mathbb{K}$ *dans lequel :*

$$\forall a, b \in \mathbb{K},\ a \times b = b \times a$$

Définition 3 :

Un ***diviseur de zéro*** *d'un anneau commutatif* $\mathbb{A}$ *est un élément non-nul* a *de* $\mathbb{A}$ *tel qu'il existe* b *non-nul et* $a \times b = 0$ *:*

$$a \in \mathbb{A}^*, \exists b \in \mathbb{A}^*,\ a \times b = 0_{\mathbb{A}}$$

Théorème 1 :

Un corps commutatif n'admet aucun diviseur de zéro.

Preuve 1.1 :

Soit $\mathbb{K}$ *un corps commutatif.*
Supposons par l'absurde que a *est un diviseur de zéro.*
Donc $a \neq 0_{\mathbb{K}}$ *et* $\exists b \neq 0_{\mathbb{K}}$ *tel que* $a \times b = 0_{\mathbb{K}}$
$a \neq 0_{\mathbb{K}} \implies a \in \mathbb{K}^\times$ *donc* $a \times b = 0_{\mathbb{K}} \implies a^{-1} \times a \times b = a^{-1} \times 0_{\mathbb{K}} \implies b = 0_{\mathbb{K}}$
Ce qui est faux par définition.

■

Définition 4 :

La ***caractéristique*** *d'un corps commutatif* $\mathbb{K}$ *est le plus petit entier naturel non-nul* n *tel que*

$$n \cdot 1_{\mathbb{K}} = 0$$

S'il n'existe pas de tel entier, on dit que la caractéristique vaut 0.

Théorème 2 :

La caractéristique d'un corps commutatif est soit 0*, soit un nombre premier.*

Preuve 2.1 :

Soit $\mathbb{K}$ *un corps commutatif. Supposons par l'absurde que* $\mathbb{K}$ *a une caractéristique* n *non-nulle et non-première, i.e.* $n = p \times q$ *avec* $p, q \notin \{0, 1\}$
Donc $n \cdot 1_{\mathbb{K}} = 0 \implies (p \times q) \cdot 1_{\mathbb{K}} = 0 \implies p \cdot 1_{\mathbb{K}} \times q \cdot 1_{\mathbb{K}} = 0 \implies p \cdot 1_{\mathbb{K}} = 0$ *ou* $q \cdot 1_{\mathbb{K}} = 0$ *car* $\mathbb{K}$ *est un corps commutatif et n'admet donc pas de diviseur de zéro.*
Ce qui contredit la minimalité de n*.*

■

Définition 5 :

Un ***corps fini*** *est un corps de cardinal fini*[1]*.*

Théorème 3 : *(admis)*

Un corps fini est commutatif.

1. On peut notamment citer les $\mathbb{Z}/p\mathbb{Z}$ avec p premier comme corps finis assez connus. Ils sont de cardinal p, et nous les noterons $\mathbb{F}_p$.

Théorème 4 *: (admis)*
Un corps fini est cyclique.

Théorème 5 *:*
Un corps fini admet une caractéristique non-nulle.

Preuve 5.1 *:*
Soit $\mathbb{K}$ un corps fini. Supposons par l'absurde que $\mathbb{K}$ a une caractéristique nulle, i.e.
$\forall n \in \mathbb{N}^*,\ n \cdot 1_{\mathbb{K}} \neq 0$
Considérons l'application

$$\theta \quad : \quad \mathbb{N} \longrightarrow \mathbb{K}$$

$$n \longmapsto n \cdot 1_{\mathbb{K}}$$

$Ker(\theta) = 0$ puisque la caractéristique est nulle. Donc θ est injective et donc $\mathbb{K}$ a au moins le même nombre d'éléments que $\mathbb{N}$ qui en a une infinité.
Ce qui contredit la finitude de $\mathbb{K}$.

■

Théorème 6 *:*
Un corps fini $\mathbb{K}$ de caractéristique p vérifie la relation suivante :

$$\forall a, b \in \mathbb{K},\ (a+b)^p = a^p + b^p$$

Preuve 6.1 *:*
Rappelons la formule du binôme de Newton (qui est valable sur les anneaux commutatifs seulement) :
Soit $\mathbb{A}$ un anneau commutatif,

$$\forall x, y \in \mathbb{A},\ (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Et la formule des coefficients binomiaux :

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Appliquons-les à notre corps fini qui est commutatif, et à la bonne puissance :

$$\forall a, b \in \mathbb{K},\ (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

avec donc

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

Or si $k \notin \{0, p\}$ alors $0 < k, p-k < p$ et puisque p est premier, $p \nmid k!(n-k)!$ donc $p \mid \frac{p!}{k!(p-k)!}$ donc $p \mid \binom{p}{k}$.
Mais $p \cdot 1_{\mathbb{K}} = 0$, donc $\forall k \in]\!]0; p[\![, \binom{p}{k} x^k y^{p-k} = 0_{\mathbb{K}}$
Concentrons-nous maintenant sur le cas $k = 0$ ou $k = p$:
$\binom{p}{0} = \binom{p}{p} = 1$.
Donc on a bien que $\forall a, b \in \mathbb{K},\ (a+b)^p = a^p + b^p$.

■

Théorème 7 :

Un corps fini $\mathbb{K}$ de caractéristique p vérifie la relation suivante :

$$\forall a, b \in \mathbb{K}, \forall n \in \mathbb{N} | (a+b)^{p^n} = a^{p^n} + b^{p^n}$$

Preuve 7.1 :

On le montre assez aisément par récurrence.

Définition 6 :

*Le **sous-corps premier** d'un corps est l'intersection de tous ses sous-corps. C'est le plus petit sous-corps du corps.*

Théorème 8 :

Un corps fini $\mathbb{K}$ de caractéristique p admet, comme sous-corps premier, $\mathbb{F}_p$, à un isomorphisme près.

Preuve 8.1 :

Définissons l'application

$$\begin{array}{ccccc} \theta & : & \mathbb{F}_p & \longrightarrow & \mathbb{K} \\ & & & & \\ & & n & \longmapsto & n \cdot 1_{\mathbb{K}} \end{array}$$

Montrons que θ est un morphisme de corps :

— $\forall a, b \in \mathbb{F}_p,\ \theta(a) + \theta(b) = a \cdot 1_{\mathbb{K}} + b \cdot 1_{\mathbb{K}} = (a+b) \cdot 1_{\mathbb{K}} = \theta(a+b)$
— $\forall a, b \in \mathbb{F}_p,\ \theta(a) \cdot \theta(b) = a \cdot 1_{\mathbb{K}} \cdot b \cdot 1_{\mathbb{K}} = (a \cdot b) \cdot 1_{\mathbb{K}} = \theta(a \cdot b)$
— $\theta(1) = 1 \cdot 1_{\mathbb{K}} = 1_{\mathbb{K}}$
— $\theta(1) = 1 \implies \forall a \in \mathbb{F}_p,\ \theta(a \cdot a^{-1}) = 1_{\mathbb{K}} \implies \theta(a) \cdot \theta(a^{-1}) = 1_{\mathbb{K}} \implies \theta(a^{-1}) = \theta(a)^{-1}$

Montrons maintenant que θ est injective :

$$\begin{aligned} \theta(a) = \theta(b) &\implies \theta(a) - \theta(b) = 0 \\ &\implies \theta(a-b) = 0 \\ &\implies (a-b) \cdot 1_{\mathbb{K}} = 0 \\ &\implies a - b \mid p \ car\ char(\mathbb{K}) = p \\ &\implies a = b \mod p \end{aligned}$$

h varie de 1 à p donc $|\theta(\mathbb{F}_p)| = p$ (puisque θ est injective) donc θ est un isomorphisme de $\mathbb{F}_p$ dans un sous-corps de $\mathbb{K}$.

On voit que ce sous-corps est de cardinal p et que donc ce sous-corps sera le sous-corps premier de $\mathbb{K}$ puisque $1_{\mathbb{K}}$ appartient à ce sous-corps stable par addition.

■

Théorème 9 :

Un corps fini $\mathbb{K}$ de caractéristique p a pour ordre une puissance de p.

Preuve 9.1 :

D'après le théorème précédent, $\mathbb{F}_p$ est un sous-corps premier de $\mathbb{K}$, donc $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectoriel, de dimension finie que l'on note n.

On a donc $|\mathbb{K}| = |\mathbb{F}_p^{dim_{\mathbb{F}_p}\mathbb{K}}| = |\mathbb{F}_p|^{dim_{\mathbb{F}_p}\mathbb{K}} = p^n$

■

Théorème 10 *: (admis)*

Soient $\mathbb{K}$ un corps commutatif, $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P.
Alors $(X - \alpha) \mid P(X)$.

Définition 7 *:*

Soient $\mathbb{K}$ un corps commutatif, $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.
*On appelle **multiplicité** de α dans P le plus grand entier e tel que $(X - \alpha)^e \mid P(X)$.*

Définition 8 *:*

Soient $\mathbb{K}$ un corps commutatif, $P \in \mathbb{K}[X]$ et $f \in \mathbb{K}[X]$ un irréductible.
*On appelle également **multiplicité** de f dans P le plus grand entier e tel que $f^e \mid P(X)$.*

Définition 9 *:*

Soient $\mathbb{K}$ un corps commutatif, $\mathbb{F}$ un sous-corps de $\mathbb{K}$ et $\alpha \in \mathbb{K}$.
On appelle polynôme minimal de α dans $\mathbb{F}[X]$ le polynôme non-nul unitaire de plus petit degré s'annulant en α [2].

Théorème 11 *:*

Soient $\mathbb{K}$ un corps commutatif, $\mathbb{F}$ un sous-corps de $\mathbb{K}$ et $\alpha \in \mathbb{K}$.
Le polynôme minimal de α dans $\mathbb{F}[X]$ est irréductible dans $\mathbb{F}[X]$.

Preuve 11.1 *:*

Supposons par l'absure que le polynôme minimal de α dans $\mathbb{F}[X]$, noté m_α, n'est pas irréductible, i.e. $\exists P, Q \in \mathbb{F}[X] \backslash \mathbb{F}[X]^\times$ tels que $m_\alpha = P \times Q$.

$$m_\alpha(\alpha) = 0 \implies P(\alpha) \times Q(\alpha) = 0 \implies \begin{cases} P(\alpha) = 0 \\ ou \\ Q(\alpha) = 0 \end{cases}$$

Ce qui contredit la minimalité du degré de m_α.

■

Théorème 12 *:*

Soient $\mathbb{K}$ un corps commutatif, $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P.
Alors α est de multiplicité 1 si et seulement si α n'est pas racine de P'.

Preuve 12.1 *:*

Conservons les mêmes notations et supposons α de multiplicté 1.
$P(\alpha) = 0 \implies P(X) = (X - \alpha) \cdot Q(X)$
$P'(X) = Q(X) + Q'(X)(X - \alpha)$
$P'(\alpha) = Q(\alpha) + Q'(\alpha) \cdot 0 = Q(\alpha)$
Puisque α est de multiplicité 1, $Q(\alpha) \neq 0$, donc α n'est pas racine de P'.

Supposons maintenant que α n'est pas racine de P'.
$P(\alpha) = 0 \implies \exists m \geq 1 \ tq \ P(X) = (X - \alpha)^m \cdot Q(X)$ *et* $(X - \alpha) \nmid Q(X)$
$P'(X) = m \cdot (X - \alpha)^{m-1} \cdot Q(X) + Q'(X) \cdot (X - \alpha)^m$
Si $m \geq 2$:
$P'(\alpha) = m \cdot (\alpha - \alpha)^{m-1} \cdot Q(\alpha) + Q'(\alpha) \cdot (\alpha - \alpha)^m = 0 + 0 = 0$
Faux par hypothèse.
Donc $m = 1$.

■

2. Dans la suite du mémoire, nous considérerons les polynômes minimaux d'un corps fini de cardinal p^n dans $\mathbb{F}_p[X]$.

Définition 10 *:*

Soient $\mathbb{K}$ un corps commutatif, et $P \in \mathbb{K}[X]$.

On appelle ***corps de décomposition*** *de P le plus petit corps contenant toutes ses racines.*

En notant $\theta_1, ..., \theta_n$ les racines de P, le corps de décomposition de P est en fait $\mathbb{K}(\theta_1 \ ... \ \theta_n)$.

Théorème 13 *: (admis)*

Soient $\mathbb{K}$ un corps commutatif, et $P \in \mathbb{K}[X]$.

Alors le corps de décomposition de P est unique à isomorphisme près.

Théorème 14 *:*

$\forall n \in \mathbb{N}^*, \forall p$ premier, il existe un corps à p^n éléments.

Preuve 14.1 *:*

Considérons le polynôme $P(X) = X^{p^n} - X$ dans $\mathbb{F}_p[X]$.

Notons $\mathbb{F}$ le corps de décomposition de P.

$P'(X) = p^n X^{p^n - 1} - 1 = -1$ n'a pas de racine, donc par le théorème précédent, toutes les racines de P sont uniques et distinctes et se trouvent dans $\mathbb{F}$.

Considérons maintenant l'ensemble de ces racines : $\mathbb{K} = \{a | a^{p^n} = a, a \in \mathbb{F}\}$. (On notera que $|\mathbb{K}| = p^n$.)

On montre facilement que $\mathbb{K}$ est un sous-corps de $\mathbb{F}$:

— $0_{\mathbb{F}}^{p^n} = 0_{\mathbb{F}}$ *donc* $0_{\mathbb{F}} \in \mathbb{K}$

— $\forall a, b \in \mathbb{K}, \ (a-b)^{p^n} = a^{p^n} + (-b)^{p^n} = a - b$ *donc* $a - b \in \mathbb{K}$

— $1_{\mathbb{F}}^{p^n} = 1_{\mathbb{F}}$ *donc* $1_{\mathbb{F}} \in \mathbb{K}$

— $\forall a, b \in \mathbb{K}, \ (ab^{-1})^{p^n} = a^{p^n}(b^{-1})^{p^n} = a(b^{p^n})^{-1} = ab^{-1}$ *donc* $ab^{-1} \in \mathbb{K}$

Donc on a bien que $\mathbb{K}$ est un corps d'ordre p^n.

■

Théorème 15 *:*

Soit $\mathbb{K}$ un corps fini de caractéristique p.

$X^{p^n} - X = \prod_{\alpha \in \mathbb{K}} (X - \alpha)$

Preuve 15.1 *:*

On sait que $X^{p^n} - X$ a au plus p^n racines. De plus, on sait que $\forall \alpha \in \mathbb{K}, \ \alpha^{p^n} = \alpha$.

Chacun des p^n éléments de $\mathbb{K}$ est racine de notre polynôme, qui a donc exactement p^n racines.

Puisque les deux polynômes ont le même coefficient dominant, on a bien

$$X^{p^n} - X = \prod_{\alpha \in \mathbb{K}} (X - \alpha)$$

■

Théorème 16 *:*

$\forall n \in \mathbb{N}^*, \forall p$ premier, il existe un unique corps à p^n éléments, à un isomorphisme près.

Preuve 16.1 *:*

Soient $\mathbb{F}$ et $\mathbb{F}'$ deux corps à p^n éléments.

On peut dire que $\prod_{\alpha \in \mathbb{F}} (X - \alpha) = X^{p^n} - X = \prod_{\beta \in \mathbb{F}'} (X - \beta) = P(X)$

Considérons maintenant une racine primitive de P dans $\mathbb{F}$, i.e.un élément a de $\mathbb{F}$ tel que $P(a) = 0$ et $ordre(a) = p^n - 1$ (a est un générateur du groupe multiplicatif de $\mathbb{F}$), et son polynôme minimal m.

On a $m \mid P$ puisque P s'annule en a, donc $\exists Q(X) \in \mathbb{F}[X]$ tq $P(X) = m(X) \cdot Q(X)$ mais $P(X) = \prod_{\beta \in \mathbb{F}'} (X - \beta)$, donc $m(X) = \prod_i (x - \beta_i)$ avec $\beta_i \in \mathbb{F}'$.

Choisissons un des β_i et notons-le b.
On sait que m est également le polynôme minimal de b puisque m est irréductible (et annule b).
Montrons que b est racine primitive dans $\mathbb{F}'$:
Supposons par l'absurde que ordre(b) = d < $p^n - 1$

$$\begin{aligned} b^d - 1 = 0 &\implies b \text{ est racine de } X^d - 1 \\ &\implies m \mid X^d - 1 \\ &\implies a \text{ est racine de } X^d - 1 \\ &\implies a^d - 1 = 0 \end{aligned}$$

Contradiction puisque ordre(a) = $p^n - 1$.
Nous pouvons donc définir une bijection θ comme :

$$\begin{array}{ccc} \theta & : & \mathbb{F} \longrightarrow \mathbb{F}' \\ & & a^i \longmapsto b^i \end{array}$$

en la complétant par $\theta(0) = 0$.
Montrons que c'est bien un morphisme :

Soient $x, y \in \mathbb{F}$.
— *$x + y = a^i + a^j = a^k$ pour un certain i, j, k.*
Donc a est racine de $Q(X) = X^i + X^j - X^k$ donc $m \mid Q$, mais on a choisi b tel que b soit racine de m, donc $Q(b) = 0$ donc b est également solution de Q et donc $b^i + b^j = b^k$
On a donc que $\theta(x + y) = \theta(a^i + a^j) = \theta(a^k) = b^k = b^i + b^j = \theta(a^i) + \theta(a^j) = \theta(x) + \theta(y)$
— *$\theta(1) = \theta(a^{p^n - 1}) = b^{p^n - 1} = 1$*
— *$\theta(x \cdot y) = \theta(a^i \cdot a^j) = \theta(a^{i+j}) = b^{i+j} = b^i \cdot b^j = \theta(a^i) \cdot \theta(a^j) = \theta(x) \cdot \theta(y)$*

C'est donc un morphisme, et évidemment un isomorphisme, donc tous les corps de même cardinal sont isomorphes entre eux.

■

Théorème 17 :
Soient $\mathbb{K}$ un corps de cardinal p^n et $\mathbb{F}$ un corps de cardinal p^m.
$\mathbb{F}$ est isomorphe à un sous-corps de $\mathbb{K}$ si et seulement si $m \mid n$.

Preuve 17.1 :
Soient $\mathbb{K}$ un corps de cardinal p^n et $\mathbb{F}$ un corps de cardinal q^m avec q et p premiers, et m et n des entiers strictements positifs.
Supposons que $\mathbb{F}$ est isomorphe à un sous-corps de $\mathbb{K}$, et notons $\tilde{\mathbb{F}}$ ce sous-corps de $\mathbb{K}$.
On sait que q = p puisque $\mathbb{F}$ admet le même sous-corps premier que $\mathbb{K}$ qui est $\mathbb{F}_p$.
On a, d'après le théorème de Lagrange, que :
$Card(\mathbb{F}^*) = Card(\tilde{\mathbb{F}}^*) \mid Card(\mathbb{K}^*) \implies p^m - 1 \mid p^n - 1 \implies m \mid n$

Soient deux entiers non-nuls m et n tels que $m \mid n$, p un nombre premier et $\mathbb{K}$ un corps de cardinal p^n.
Considérons $\mathbb{F} = \{x \in \mathbb{K} | x^{p^m} = x\}$.
Montrons que $\mathbb{F}$ est un sous-corps de $\mathbb{K}$:
— *$0_{\mathbb{K}}$ et $1_{\mathbb{K}} \in \mathbb{F}$ évidemment.*
— *$\forall a, b \in \mathbb{F}, (a + b)^{p^m} = a^{p^m} + b^{p^m} = a + b$, donc $a + b \in \mathbb{F}$.*

— $\forall a, b \in \mathbb{F}, (a \times b)^{p^m} = a^{p^m} \times b^{p^m} = a \times b$, *donc* $a \times b \in \mathbb{F}$.
— $\forall a \in \mathbb{F}^*, (a^{-1})^{p^m} = (a^{p^m})^{-1} = a^{-1}$, *donc* $a^{-1} \in \mathbb{F}$.
Donc $\mathbb{F}$ *est un sous-corps de* $\mathbb{K}$.

Calculons maintenant le cardinal de $\mathbb{F}$ *:*
$m \mid n \implies X^m - 1 \mid X^n - 1 \implies p^m - 1 \mid p^n - 1 \implies X^{p^m-1} - 1 \mid X^{p^n-1} - 1 \implies X^{p^m} - X \mid X^{p^n} - X$.
Mais sachant que $X^{p^n} - X = \prod_{\alpha \in \mathbb{K}} (X - \alpha)$, *on a que* $X^{p^m} - X = \prod_{\alpha_i \in \mathbb{K}} (X - \alpha_i)$ *avec* $1 \leq i \leq p^m$ *pour respecter le degré, et* $i \neq j \implies \alpha_i \neq \alpha_j$.

Donc on a bien que $\mathbb{F}$ *a* p^m *éléments.*

■

2 L'algorithme de Cantor-Zassenhaus

Nous allons donc voir un algorithme permettant de factoriser dans $\mathbb{F}_p[X]$, qui nous sert notamment dans la cryptographie par bloc. Cet algorithme a été trouvé par *David Cantor* et *Hans Julius Zassenhaus* en 1981, après qu'*Elwyn Berlekamp* en ait trouvé un en 1967.

Cet algorithme peut facilement être adapté à des corps finis quelconques, i.e. avec un cardinal de p^n, pour tout nombre premier p et tout entier non-nul n.

Une des particularités de cet algorithme est qu'il fonctionne uniquement sur des polynômes sans facteurs carrés (c'est-à-dire que la multiplicté des polynômes irréductibles est inférieure ou égale à 1), et dont les polynômes irréductibles qui le composent sont tous de même degré, contrairement à celui de *Berlekamp* qui fonctionne sur des polynômes sans facteurs carrés, mais dont les irréductibles peuvent être de différents degrés. C'est pourquoi l'algorithme de *Cantor-Zassenhaus* se compose de trois étapes :

— La première consiste à décomposer notre polynôme de base en polynômes sans facteurs carrés.
— La deuxième à décomposer nos polynômes sans facteurs carrés en polynômes d'irréductibles de même degré.
— Et la troisième qui factorise à proprement parler.

2.1 Première Étape

La première étape consiste donc à supprimer les facteurs carrés d'abord. Pour cela, nous allons faire le $pgcd(P, P')$, ce qui nous donnera soit P, soit un autre polynôme, que l'on nommera Q.

Si l'on a P, on recommence la première étape avec la racine p-ème de P, sinon, on "sauvegarde" le polynôme $\frac{P}{Q}$ qui sera sans facteur carré, et on recommence avec Q.

2.2 Deuxième Étape

La deuxième étape consiste à isoler les produits des polynômes irréductibles de même degré. On va, pour ce faire, calculer $pgcd(P, X^{p^i} - X)$ qui va être égal au produit des irréductibles de P de degré i. On répète cette étape récursivement, jusqu'à ne plus rien avoir à séparer.

2.3 Troisième Étape

Nous allons voir ici une première méthode pour factoriser des polynômes à coefficients dans un corps fini de caractéristique impair, et une deuxième pour ceux de caractéristique paire. En effet, la première méthode ne marche pas pour les carcatéristiques paires (nous verrons pourquoi dans la correction de l'algorithme), et la deuxième est trop coûteuse en temps pour l'appliquer aux caractéristiques impaires.

2.3.1 Caractéristique impaire

La partie principale de l'algorithme consiste à choisir un polynôme U aléatoirement parmi ceux de degré strictement inferieur au polynôme P que l'on veut factoriser. Et calculer successivement

— $pgcd(P, U^{\frac{p^i-1}{2}} - 1)$

— $pgcd(P, U^{\frac{p^i-1}{2}} + 1)$

— $pgcd(P, U)$

en espérant être tombé sur un U qui permet de factoriser non-trivialement P (avoir un *pgcd* différent de 1 ou de P).

Si jamais un des *pgcd* n'est pas trivial, nous recommençons sur chaque nouveau polynôme jusqu'à avoir uniquement des polynômes de degré i.

Si jamais tous les *pgcd* sont triviaux, nous choisissons un autre U et nous recommençons.

2.3.2 Caractéristique paire

Le principe de cette étape reste le même que celui pour une caractéristique impaire, nous tirons toujours un polynôme U aléatoire de degré strictement inferieur au degré du polynôme que l'on veut factoriser. La seule différence est le polynôme par lequel nous faisons le pgcd. Nous allons, cette fois-ci, faire :

— $pgcd(P, U + U^p + U^{p^2} + \cdots + U^{p^{deg(P)-1}})$

en espérant toujours être tombé sur un polynôme qui nous permet de factoriser P. Si c'est le cas, on recommence avec le *pgcd* et le quotient de P par le *pgcd*. Si ce n'est pas le cas, nous recommençons l'étape avec un autre U.

Notons que calculer des puissances de polynômes, et des *pgcd* de polynômes peut prendre beaucoup de temps si les polynômes sont grands. Ce qui est notre cas puisque nous élevons plus ou moins à des puissance une puissance de p des polynômes. Pour pallier à ce problème, nous utilisons l'exponentiation rapide, et nous calculons ces puissances dans l'anneau de nos polynômes, quotienté par P (le premier argument des *pgcd*), ce qui nous permet d'élever à une certaine puissance plus rapidement, et de toujours revenir à un polynôme de degré inferieur à celui de P.

2.4 Un peu de code

L'algorithme présenté ci-dessus peut être implémenté assez facilement (comme ci-dessous) [3] :

Commençons par la première étape.

```
def PremiereEtape(P,L,mult):
    if(P.degree()==0): #P est une constante, on ne s'en préoccupe pas
        return L
    if(P.degree()==1):
        L.append([mult,P]) #P est de degré 1, donc forcément sans facteurs carrés
        return L
    p=P.parent().characteristic() #p est la caractéristique de notre ensemble
    Q=gcd(P,P.derivative()) #Le pgcd de P et P'
    if Q==P :
        return PremiereEtape(RacinePeme(P),L,mult*p) #On recommence avec la racine p-ème de P
    else :
        L.append([mult,P//Q]) #On "sauvegarde" P/Q (qui est sans facteurs carrés)
        return PremiereEtape(Q,L,1) #Et on recommence avec le reste
```

On continue avec la deuxième étape.

```
def DeuxiemeEtape(P):
    p=P.parent().characteristic()
    L=[]
    i=1 #Le degré des polynômes irréductibles qu'on veut extraire de P
    mod=P.parent().quotient(P) #L'anneau des polynômes auquel P appartient
                               #quotienté par P (afin d'éviter de calculer
                               #des polynômes trop grands)
    while P.degree()!=0 :
        L.append(gcd(P,lift(ExpRapide(mod(x),ExpRapide(p,i))-x))) #On utilise l'exponentiation
                                                                  #rapide (afin d'aller
                                                                  #plus vite)
        P=P//L[i-1] #On divise par les irréductibles de degré i qui composent P
        i=i+1 #Et on recommence
    return L
```

3. Le code sans commentaire est en annexe à la fin du mémoire

Et on finit avec la troisième étape (pour une caractéristique impaire).

```
def TroisiemeEtape(P,i,L):
    if(P.degree()==i):  #On a un polynôme de degré i donc un polynôme irréductible
        L.append(P)     #Donc on l'ajoute à notre liste
        return L

    p=P.parent().characteristic()
    U=Al(P)     #Un polynôme aléatoire de dgré strictement inferieur à celui de P
    r=(ExpRapide(p,i)-1)//2
    mod=P.parent().quotient(P)

    Q1=gcd(P,lift(ExpRapide(mod(U),r)-1))
    if(Q1==P):                          #La factorisation est triviale
        return TroisiemeEtape(P,i,L)    #On recommence

    Q2=gcd(P,lift(ExpRapide(mod(U),r)+1))
    if(Q2==P):                          #La factorisation est triviale
        return TroisiemeEtape(P,i,L)    #On recommence

    Q3=gcd(P,U)
    if(Q3==P):                          #La factorisation est triviale
        return TroisiemeEtape(P,i,L)    #On recommence

    if(Q1!=1):
        TroisiemeEtape(Q1,i,L)

    if(Q2!=1):
        TroisiemeEtape(Q2,i,L)

    if(Q3!=1):
        TroisiemeEtape(Q3,i,L)

    return L
```

Et celle pour une caractéristique paire.

```
def TroisiemeEtapeBis(P,i,L):
    if(P.degree()==i):
        L.append(P)
        return L

    p=P.parent().characteristic()
    U=Al(P)
    mod=P.parent().quotient(P)
    Q=SommePolPuiss(mod(U),P)       #On calcule le polynôme avec les puissances de p
                                    #efficacement encore une fois grace à l'exponentitation
                                    #rapide et le modulo
    Q1=gcd(P,lift(Q))
    if(Q1==P):                          #La factorisation est triviale
        return TroisiemeEtape(P,i,L)    #On recommence

    TroisiemeEtape(Q1,i,L)
    TroisiemeEtape(P//Q1,i,L)
    return L
```

On peut donc finaliser notre algorithme entier comme ce qui suit.

```
def CantorZassenhaus(P):
    Liste=[]        #La liste qui contiendra tous nos facteurs, et leur multiplicité
    for [mult,PolSansFacCar] in PremiereEtape(P,[],1): #La liste des facteurs de P sans
                                                       # facteurs carrés
        L=DeuxiemeEtape(PolSansFacCar)      #La liste des polynômes dont tous les irréductibles
                                            #sont de même degré pour un polynôme sans
                                            #facteur carré donné
        for i in range(len(L)):
            if(L[i]!=1):
                if (P.parent().characteristic()==2):        #La caractéristique est paire, on
                                                            #applique la deuxième version de la
                                                            #troisième étape
                    for pol in TroisiemeEtapeBis(L[i],i+1,[]):
                        Liste=Ajout(pol,mult,Liste)
                else :                                      #La caractéristique est impaire, on
                                                            #applique la première version de la
                                                            #troisième étape
                    for pol in TroisiemeEtape(L[i],i+1,[]): #L'étape principale appliquée à
                                                            #chaque polynôme sans facteur carré
                                                            #dont tous les irréductibles sont
                                                            #de même degré
                        Liste=Ajout(pol,mult,Liste)
    return Liste
```

3 Correction de l'algorithme

3.1 Première étape

Commençons par la première étape, la suppression des facteurs carrés :

Théorème 18 *:*

Soient $\mathbb{K}$ un corps fini de caractéristique p et A un polynôme de $\mathbb{K}[X]$, alors
Soit

$$\exists B \in \mathbb{K}[X] \text{ tel que } A = B^p$$

Soit

$$\frac{A}{pgcd(A, A')} \text{ est sans facteurs carrés}$$

Preuve 18.1 *:*

A se décompose en produit de puissances d'irréductibles donc on peut écrire $A = \prod_i f_i^{e_i}$.

Concentrons-nous sur un des polynômes irréductibles, que l'on notera f, et dont la multiplicité sera e : on peut écrire $A = f^e \cdot B$ avec $pgcd(f^e, B) = 1$.
On a $A' = ef^{e-1}f'B + f^eB'$.
Regardons la multiplicté de f dans A' (notée $mult_{A'}(f)$) :
$mult_{A'}(f) \geq e - 1$ car $A' = f^{e-1}(ef'B + fB')$.
Regardons quand est-ce que la multiplicité de f dans A' est plus grande que e :

$$mult_{A'}(f) \geq e \implies f | ef'B + fB' \implies f | ef'B \implies f | ef' \implies \begin{cases} e = 0 \mod p \\ ou \\ f' = 0 \end{cases}$$

car $deg(f) > deg(f')$.
Notons $f = \sum a_i X^i$ et donc $f' = \sum i a_i X^{i-1}$.

$$f' = 0 \Leftrightarrow \forall i, \begin{cases} i = 0 \mod p \\ ou \\ a_i = 0 \mod p \end{cases}$$

Si $\forall i,\ a_i = 0 \mod p$, alors $f = 0$ et f n'est donc pas irréductible.
Donc $\forall i,\ a_i \neq 0 \implies i = 0$ et on sait qu'il existe un i tel que $a_i \neq 0$.
Donc $f = \sum a_{ip} X^{ip} = (\sum \sqrt[p]{a_{ip}} X^i)^p$, ce qui contredit l'irréductibilité de f donc f' ne peut être nul et donc on a que $e = 0 \mod p$.
Donc en notant $A = \prod_i f_i^{e_i}$, on a que

$$mult_{A'}(f_i) \begin{cases} \geq e_i & si\ e_i = 0 \mod p \\ = e_i - 1 & sinon \end{cases}$$

Donc $pgcd(A, A') = \prod_{\substack{i \\ e_i | p}} f_i^{e_i - 1} \times \prod_{\substack{j \\ e_j \nmid p}} f_j^{e_j}$.
On note que si $\forall i,\ e_i = 0 \mod p, \exists B$ tq $A = B^p$ et $pgcd(A, A') = A$ (car $A' = 0$), c'est ce B qui est considéré comme la racine p-ème de A.

Supposons maintenant que $A \neq B^p$, alors on a

$$\frac{A}{pgcd(A, A')} = \prod_{\substack{i \\ e_i | p}} f_i$$

■

On voit bien qu'en réitérant cet algorithme sur les *pgcd* successifs, et en retenant le nombre de fois que l'on a fait "racine p-ième", on décompose notre polynôme de base en polynômes sans facteurs carrés.

3.2 Deuxième étape

Théorème 19 *:*

$X^{p^n} - X = \prod f$ avec f parcourant l'ensemble des polynômes irréductibles unitaires de degré divisant n.

Preuve 19.1 [4] *:*

Soit f un polynôme irréductible, unitaire de degré m divisant n.

On peut construire un corps $\mathbb{F}$ à p^m élément en quotientant $F_p[X]$ par f. Et notons $\alpha = X \mod f$.

On observe que dans $\mathbb{F}[X]$, le polynôme minimal de α est f, et que puisque α appartient à un corps de cardinal p^m, α vérifie $\alpha^{p^m} - \alpha = 0$.

On en déduit que $f \mid X^{p^m} - X$.

De plus, considérons un corps $\mathbb{K}$ de cardinal p^n. On sait que $\mathbb{F}$ est isomorphe à un sous-corps $\tilde{\mathbb{F}}$ de $\mathbb{K}$, ce qui implique que $\forall a \in \tilde{\mathbb{F}}$, $a^{p^n} - a = 0$, donc tous les éléments de $\tilde{\mathbb{F}}$ sont racines de $X^{p^n} - X$ (et aussi de $X^{p^m} - X$).

Donc on a $X^{p^m} - X \mid X^{p^n} - X$, et donc $f \mid X^{p^n} - X$.

Puisque tous les irréductibles sont premiers entre eux, on a $\prod f \mid X^{p^n} - X$.

Soit $\mathbb{K}$ un corps de cardinal p^n.

Rappelons que $X^{p^n} - X = \prod_{a \in \mathbb{K}} (X - a)$.

Considérons f un polynôme irréductible divisant $X^{p^n} - X$, soient α une racine de f dans $\mathbb{K}$ et m le degré de f.

Considérons le sous-corps de $\mathbb{K}$ engendré par α : $\mathbb{F}_p(\alpha)$,

et l'application :

$$\theta \quad : \quad \mathbb{F}_p[X] \longrightarrow \mathbb{F}_p(\alpha)$$

$$P(X) \longmapsto P(\alpha).$$

$Ker(\theta) = \{P \in \mathbb{F}[X]; P(\alpha) = 0\} = \{P \in \mathbb{F}[X]; f \mid P\} = (f)$.

Donc on a $\mathbb{F}_p[X]/(f) = \mathbb{F}_p[X]/Ker(\theta) \simeq Im(\theta) = \mathbb{F}_p(\alpha)$ qui est un sous-corps de $\mathbb{K}$.

$deg(f) = m$ donc $Card(\mathbb{F}_p(\alpha)) = p^m$ et donc $m \mid n$.

On en déduit que $X^{p^n} - X$ se factorise en produit de polynômes irréductibles de degré divisant n (on peut facilement supposer qu'ils sont unitaires).

Donc on a évidemment que $X^{p^n} - X \mid \prod f$ avec f parcourant l'ensemble des polynômes irréductibles unitaires de degré divisant n.

De plus, $X^{p^n} - X$ et $\prod f$ avec f parcourant l'ensemble des polynômes irréductibles unitaires de degré divisant n ont le même coefficient dominant, donc $X^{p^n} - X = \prod f$ avec f parcourant l'ensemble des polynômes irréductibles unitaires de degré divisant n.

■

4. Nous nous basons, pour cette preuve, sur le fait que $m \mid n \Leftrightarrow X^m - X \mid X^n - X$. C'est un résultat connu, que nous ne démontrerons pas ici.

Donc en faisant $pgcd(A, X^{p^i} - X)$ pour chaque i jusqu'à ne plus rien avoir, on se rend bien compte qu'on décompose en fait notre polynôme A non pas en produit de polynômes irréductibles, unitaires de degré divisant i, mais bien en produit de polynômes irréductibles, unitaires de degré i (puisque l'on commence à 1, les diviseurs de i sont déjà "sortis").

3.3 Troisième étape

3.3.1 Caractéristique impaire

Remarquons que $X^{p^d} - X = X \cdot (X^{p^d-1} - 1) = X \cdot ((X^{\frac{p^d-1}{2}})^2 - 1^2) = X \cdot (X^{\frac{p^d-1}{2}} - 1) \cdot (X^{\frac{p^d-1}{2}} + 1)$. Cette formule n'a de sens que si p^d est impair, et donc p impair. Nous supposons donc p impair, et nous traiterons le cas p pair ultérieurement.

On sait que $X^{p^d} - X$ est le produit de tous les polynômes **irréductibles** unitaires de degré divisant d, donc

$$pgcd(X, X^{\frac{p^d-1}{2}} - 1) = pgcd(X, X^{\frac{p^d-1}{2}} + 1) = pgcd(X^{\frac{p^d-1}{2}} - 1, X^{\frac{p^d-1}{2}} + 1) = 1$$

Donc en supposant notre polynôme P comme produit d'irréductibles de degré d et de multiplicité 1, on a $pgcd(P, X^{p^d} - X) = P$, donc sachant que X, $X^{\frac{p^d-1}{2}} - 1$ et $X^{\frac{p^d-1}{2}} + 1$ sont premiers entre eux, on a

$$P = pgcd(P, X) \cdot pgcd(P, X^{\frac{p^d-1}{2}} - 1) \cdot pgcd(P, X^{\frac{p^d-1}{2}} + 1)$$

Théorème 20 *:*

Soient $\mathbb{K}$ un corps de cardinal p^d, $U \in \mathbb{F}_p[X]$, f un polynôme irréductible de degré d et α une racine de f.

Alors $f \mid U^{\frac{p^d-1}{2}} - 1$ si et seulement si $U(\alpha)$ est un carré non-nul dans $\mathbb{K}$.

Preuve 20.1 *:*

Supposons que $f \mid U^{\frac{p^d-1}{2}} - 1$.

Or, $f(\alpha) = 0$ donc $U(\alpha)^{\frac{p^d-1}{2}} - 1 = 0 \Leftrightarrow U(\alpha)^{\frac{p^d-1}{2}} = 1$.

Soit g un générateur de $\mathbb{K}^*$.

Supposons par l'absurde que $U(\alpha)$ n'est pas un carré, i.e. $\exists k \in \mathbb{N}$ tq $U(\alpha) = g^{2k+1}$:

$U(\alpha)^{\frac{p^d-1}{2}} = 1 \implies (g^{2k+1})^{\frac{p^d-1}{2}} = 1 \implies (g^{p^d-1})^k \cdot g^{\frac{p^d-1}{2}} = 1 \implies 1^k \cdot (-1) = 1 \implies -1 = 1$

Ce qui est bien évidemment faux, donc $U(\alpha)$ est un carré.

Supposons encore par l'absurde qu'il est nul. Nous obtenons par le même principe que $0 = 1$ ce qui est encore une fois faux. Donc $\exists k \in \mathbb{N}$ tq $U(\alpha) = g^{2k}$, autrement dit, $U(\alpha)$ est un carré non-nul dans $\mathbb{K}$.

Supposons que $U(\alpha)$ est un carré non-nul dans $\mathbb{K}$:

$$\begin{aligned} \exists y \in \mathbb{K}^* \text{ tq } U(\alpha) = y^2 &\implies U(\alpha)^{\frac{p^d-1}{2}} = (y^2)^{\frac{p^d-1}{2}} \\ &\implies U(\alpha)^{\frac{p^d-1}{2}} = y^{p^d-1} = 1 \\ &\implies U(\alpha)^{\frac{p^d-1}{2}} - 1 = 1 - 1 = 0 \end{aligned}$$

Mais, f est le polynôme minimal de α sur $\mathbb{F}_p[X]$ puisque f est irréductible, donc $f \mid U^{\frac{p^d-1}{2}} - 1$.

■

De même, on déduit que $f \mid pgcd(P, U) \Leftrightarrow U(\alpha) = 0$ et donc, par élimination, que $f \mid pgcd(P, U^{\frac{p^d-1}{2}} + 1) \Leftrightarrow U(\alpha)$ est un non-carré non-nul dans $\mathbb{K}$.

Tout d'abord, rappelons que P est un produit d'irréductibles de même degré :
$P = \prod_{i=1}^{k} f_i$ avec $deg(f_i) = d \ \forall i$ et $n = deg(P) = k \times d$

On note $\mathbb{F}_p[X]_{<n}$ l'ensemble des polynômes à coefficients dans $\mathbb{F}_p$ de degré strictement inferieur à n :

$$\mathbb{F}_p[X]_{<n} = \{Q \in \mathbb{F}_p[X] | deg(Q) < n\}$$

Et on a

$$\mathbb{F}_p[X]_{<n} \simeq \mathbb{F}_p[X]/(P) \simeq \prod_{i=1}^{k} \mathbb{F}_p[X]/(f_i)$$

par le théorème des restes chinois.

On munit cet ensemble d'une loi de probabilité uniforme.
$\mathbb{P}(U \mod f_i \text{ est un carré non-nul}) = \frac{p^d-1}{2} \times \frac{1}{p^d} = \frac{1}{2} \times (1 - \frac{1}{p^d})$

Donc les cas où le premier pgcd ne permet pas de factoriser P sont les cas où $\forall i,\ f_i \mid U^{\frac{p^d-1}{2}} - 1 \Leftrightarrow \forall i,\ U(\alpha_i)$ est un carré non-nul dans $\mathbb{K}$, en définissant α_i comme une racine de f_i.
$\mathbb{P}(\textit{le premier pgcd ne permet pas de factoriser } P) = \mathbb{P}(\forall i,\ U \mod f_i \textit{ est un carré non} - \textit{nul}) = \prod_{i=1}^{k} (\frac{1}{2} \times (1 - \frac{1}{p^d})) = (\frac{1}{2} \times (1 - \frac{1}{p^d}))^k$ car les évenements sont indépendants.

$$(\frac{1}{2} \times (1 - \frac{1}{p^d}))^k = (\frac{1}{2})^k \times (1 - \frac{1}{p^d})^k < (\frac{1}{2})^k$$

De même, la probabilité d'échec pour le deuxième *pgcd* est de $\frac{1}{2^k} \times (1 - \frac{1}{p^d})^k < (\frac{1}{2})^k$, et celle du troisième de $(\frac{1}{p^d})^k$.
La probabilité que tous les événements échouent est donc inférieure à

$$(\frac{1}{2})^k + (\frac{1}{2})^k + (\frac{1}{p^d})^k \leq (\frac{1}{2})^{k-1} + (\frac{1}{p^d})^k$$

On sait que P est composé d'au moins 2 polynômes irréductibles, sinon il n'y a pas besoin de factoriser, donc $k \geq 2$.
On sait que $d \geq 1$.
Et on sait que $p \geq 3$ par définition de p, qui est un nombre premier impair.
Donc on a :

$$\begin{array}{lll} k \geq 2 & \Longrightarrow & k - 1 \geq 1 \\ & \Longrightarrow & 2^{k-1} \geq 2 \\ & \Longrightarrow & \frac{1}{2^{k-1}} \leq \frac{1}{2} \end{array} \qquad \& \qquad \begin{array}{lll} p \geq 3 & \Longrightarrow & p^d \geq 3^1 = 3 \\ & \Longrightarrow & \frac{1}{p^d} \leq \frac{1}{3} \\ & \Longrightarrow & (\frac{1}{p^d})^k \leq (\frac{1}{3})^2 = \frac{1}{9} \end{array}$$

Ce qui nous donne que

$$(\frac{1}{2})^{k-1} + (\frac{1}{p^d})^k \leq \frac{1}{2} + \frac{1}{9} = \frac{11}{18}$$

Donc la probabilité que la troisième étape échoue k fois d'affilée est de $(\frac{11}{18})^k$ qui tend vers 0 quand k est grand.

Nous avons donc là un algorithme probabiliste qui nous factorise un polynôme P sans facteurs carrés, et dont tous les irréductibles sont de même degré.

3.3.2 Caractéristique paire

Théorème 21 *:*
Soit $T_d(X) = X + X^p + X^{p^2} + \cdots + X^{p^{d-1}}$.
Alors $X^{p^d} - X = \prod_{\alpha \in \mathbb{F}_p} (T_d(X) - \alpha)$.

Preuve 21.1 *Tout d'abord, notons que les deux polynômes ont le même coefficient dominant, et le même degré. En effet,*

$$deg(X^{p^d} - X) = p^d$$

et

$$deg(\prod_{\alpha \in \mathbb{F}_p} (T_d(X) - \alpha)) = p \times deg(T_d(X) - \alpha) = p \times p^{d-1} = p^d$$

Il nous suffit donc de montrer que l'un divise l'autre pour montrer qu'ils sont égaux.

Montrons que $X^{p^d} - X \mid \prod_{\alpha \in \mathbb{F}_p} (T_d(X) - \alpha)$.

Considérons un corps $\mathbb{K}$ *de cardinal* p^d. *On sait que* $\forall \theta \in \mathbb{K},\ \theta$ *est racine de* $X^{p^d} - X$. *Donc pour montrer la divisibilité, il nous suffit de montrer que pour tous les* p^d *éléments* $\theta \in \mathbb{K},\ \theta$ *est racine de* $\prod_{\alpha \in \mathbb{F}_p} (T_d(X) - \alpha)$, *i.e.* $\forall \theta \in \mathbb{K},\ \exists \beta \in \mathbb{F}_p$ *tel que* $T_d(\theta) = \beta$, *i.e.* $\forall \theta \in \mathbb{K},\ T_d(\theta) \in \mathbb{F}_p$.

On sait que $X^p - X$ *admet* p *racines distinctes dans* $\mathbb{F}_p$ *qui a lui-même* p *éléments. Donc* $y \in \mathbb{F}_p \Leftrightarrow y^p - y = 0$.
Donc calculons $T_d(\theta)^p$ *:*

$$T_d(\theta)^p = (\theta + \theta^p + \cdots + \theta^{p^{d-1}})^p = \theta^p + \theta^{p^2} + \cdots + \theta^{p^d} = \theta^p + \theta^{p^2} + \cdots + \theta = \theta + \theta^p + \cdots + \theta^{p^{d-1}} = T_d(\theta)$$

Donc on a bien que $T_d(\theta) \in \mathbb{F}_p$.
L'égalité est démontrée.

■

Le reste de la correction est la même que pour une caractéristique impaire.

4 Complexité

Essayons de determiner dans cette partie la complexité de notre algorithme.

Rappelons quelques complexités d'opérations élémentaires que nous utilisons dans cet algorithme :

- *pgcd* : Calculer le *pgcd* de deux polynômes A et B avec $deg(A) > deg(B)$ se fera en $deg(A)^2$ opérations.
- Exponentiation rapide : Élever x à la puissance n se fera en $log(n)$ opérations.
- Multiplication (et division) modulo p : Multiplier (ou diviser) x modulo p par y modulo p se fera en $log(p)^2$ opérations.
- Multiplication (et division) modulo P : Multiplier (et diviser) Q modulo P par S modulo P se fera en $deg(P)^2$ opérations.

Soit $A \in \mathbb{F}_p[X] \mod P$. Calucler X^n avec l'exponentiation rapide se fera en $log(n)$ opérations. Sachant que ces calculs se font modulo P et modulo p, le calcul général se fera finalement en

$$O(log(n) \times log(p)^2 \times deg(P)^2)$$

On utilise l'exponentiation rapide sur X à la deuxième étape (lorsqu'on fait $pgcd(X^{p^i} - X, P)$). On sait que $deg(P) > i$ donc on a $p^{deg(P)} > p^i$.

Donc on peut écrire

$$O(log(n) \times log(p)^2 \times deg(P)^2) = O(log(p^{deg(P)}) \times log(p)^2 \times deg(P)^2) = O(deg(f)^3 \times log(p)^3)$$

On voit donc que cette exponentiation rapide est en fait polynomiale en $deg(P)$ et en $log(p)$.

Les *pgcd* sont aussi polynômiaux en $deg(P)$ et en $log(p)$, ce qui nous donne un alogrithme général probabiliste et polynomial en $deg(P)$ et en $log(p)$.

5 Conclusion

Nous avons vu dans ce mémoire ce qu'était un corps fini, et un algorithme permettant de factoriser les polynômes à coefficients dans ces corps finis.

Cet algorithme est le meilleur connu à ce jour, il a une complexité polynomiale en *log* de la caractéristique de notre corps, et en degré du polynôme à factoriser.

Cette capacité de factorisation est donc possible, assez rapidement, dans un corps fini, mais elle reste tout de même un défi à relever dans l'anneau des entiers relatifs : $\mathbb{Z}$, puisque nous ne savons toujours pas factoriser efficacement les entiers en produit de puissances de nombres premiers dans cet anneau.

Une des forces de cet algorithme est qu'il utilise des propriétés fondamentales des corps finis, comme l'équation universelle, et des outils simples, commes les *pgcd*. On aurait aussi pu parler de l'algorithme de Berlekamp, qui se base plutôt sur des calculs matriciels et de l'algèbre linéaire, et qui a une complexité en $O(qn^3)$, avec q le cardinal de notre corps, et n le degré de notre polynôme.

Ces algorithmes de factorisation nous permettent également de reconnaitre les irréductibles des anneaux des polynômes à coefficients dans un corps fini, puisque si notre factorisation nous retourne un résultat trivial, cela implique que notre polynôme est un produit d'un inversible et d'**un** irréductible : notre polynôme de base.

Références

[1] Timothy Murphy. *Course 373-Finite Fields*. University of Dublin, Trinity College School of Mathematics ; 2006.

[2] Rudolf Lidl & Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge university press ; 1994.

[3] Jean-Marc Couveignes.

6 Annexe

```
def PremiereEtape(P,L,mult):
    if(P.degree()==0):
        return L
    if(P.degree()==1):
        L.append([mult,P])
        return L
    p=P.parent().characteristic()
    Q=gcd(P,P.derivative())
    if Q==P :
        return PremiereEtape(RacinePeme(P),L,mult*p)
    else :
        L.append([mult,P//Q])
        return PremiereEtape(Q,L,1)
```

```
def DeuxiemeEtape(P):
    p=P.parent().characteristic()
    L=[]
    i=1
    mod=P.parent().quotient(P)
    while P.degree()!=0 :
        L.append(gcd(P,lift(ExpRapide(mod(x),ExpRapide(p,i))-x)))
        P=P//L[i-1]
        i=i+1
    return L
```

```
def TroisiemeEtapeBis(P,i,L):
    if(P.degree()==i):
        L.append(P)
        return L

    p=P.parent().characteristic()
    U=Al(P)
    mod=P.parent().quotient(P)
    Q=SommePolPuiss(mod(U),P)

    Q1=gcd(P,lift(Q))
    if(Q1==P):
        return TroisiemeEtape(P,i,L)

    TroisiemeEtape(Q1,i,L)
    TroisiemeEtape(P//Q1,i,L)
    return L
```

```
def TroisiemeEtape(P,i,L):
    if(P.degree()==i):
        L.append(P)
        return L

    p=P.parent().characteristic()
    U=Al(P)
    r=(ExpRapide(p,i)-1)//2
    mod=P.parent().quotient(P)

    Q1=gcd(P,lift(ExpRapide(mod(U),r)-1))
    if(Q1==P):
        return TroisiemeEtape(P,i,L)

    Q2=gcd(P,lift(ExpRapide(mod(U),r)+1))
    if(Q2==P):
        return TroisiemeEtape(P,i,L)

    Q3=gcd(P,U)
    if(Q3==P):
        return TroisiemeEtape(P,i,L)

    if(Q1!=1):
        TroisiemeEtape(Q1,i,L)

    if(Q2!=1):
        TroisiemeEtape(Q2,i,L)

    if(Q3!=1):
        TroisiemeEtape(Q3,i,L)

    return L



def CantorZassenhaus(P):
Liste=[]
for [mult,PolSansFacCar] in PremiereEtape(P,[],1):
    L=DeuxiemeEtape(PolSansFacCar)
    for i in range(len(L)):
        if(L[i]!=1):
            if (P.parent().characteristic()==2):
                for pol in TroisiemeEtapeBis(L[i],i+1,[]):
                    Liste=Ajout(pol,mult,Liste)
            else :
                for pol in TroisiemeEtape(L[i],i+1,[]):
                    Liste=Ajout(pol,mult,Liste)
return Liste
```