Table des matières

UNIVERSITE FELIX HOUPOUET BOIGNY
Mai 2018

ECOLE DE RECHERCHE CIMPA Kinshasa 2018

Université de Kinshasa du 07 au 18 mai 2018

THEME : Arithmétique algorithmique et cryptographie

Cours : Décompositions polynomiales et quelques algorithmes de factorisation sur les corps finis

Dr Tanoé François E.

Université Félix Houphouët BOIGNY
UFR MI - Laboratoire de Mathématiques Fondamentales

email : aziz_marie@yahoo.fr

0.1 INTRODUCTION

La factorisation des polynômes est un des problèmes fondamentaux du calcul formel, sur lequel beaucoup de progrès significatifs ont été faits ces 30 dernières années. Les situations et les problèmes soulevés sont variés : avec une ou plusieurs variables, factorisation dans un anneau ou dans un corps, factorisation rationnelle ou absolue, polynômes denses, convexes-denses, complexité arithmétique ou complexité en bits, gestion cours, etc. Les techniques pour approcher ces problèmes sont variées (corps finis, algèbre linéaire, théorie des nombres, géométrique algébrique, géométrie diophantienne, algorithme, etc...)

Un des problèmes fondamentaux est la factorisation des polynômes uni-variés à coefficients dans un corps fini $\mathbb{F}_p$ ou p est un nombres premier. Ce problème a de nombreuses applications en cryptographie.
Remarquons que l'anneau $\mathbb{F}_p[X]$ est factoriel, tout polynôme univarié $P(X) \in \mathbb{F}_p[X]$ se factorise de manière unique sous la forme

$$P = cP_1^{m_1} \cdots P_s^{m_s}$$

où $c \in \mathbb{F}_p^*$, $m_i \in \mathbb{F}_p[X]$ sont des polynômes irréductibles unitaires non constants distincts deux à deux.
L'objectif de ce cours est de présenter des algorithmes qui, étant donné un polynôme $P(X) \in \mathbb{F}_p[X]$, retourne la liste $[c, (P_1, m_1), \cdots, (P_s, m_s)]$.

Dans le premier chapitre, nous définissons quelques notions de bases des anneaux, des corps, ainsi que les extensions de corps.

Dans le deuxième chapitre nous donnons quelques propriétés sur les fonctions arithmétiques, dont la formule de Möbius qui est très importante dans la détermination du nombres de polynômes unitaires et irréductibles de degré $n \in \mathbb{N}$ sur des corps finis

Dans le chapitre trois nous revenons encore sur les corps plus précisément sur les corps finis où nous présentons les résultats fondamentaux concernant les corps finis : existence, unicité, théorème de Wedderburn et le théorème de l'élément primitif. On s'intéresse ensuite a quelques propriétés relative aux polynômes irréductibles sur de tel corps

Dans le dernier chapitre nous étudions la décomposition des polynômes sur des corps finis. Pour pouvoir effectivement décomposer les polynômes sur les corps finis nous avons proposé deux algorithmes qui sont :
- L'algorithme de **Elwin R. Berlekamp** découvert en 1967. C'est un algorithme en complexité polynomiale permettant de factoriser un polynôme sur un corps fini présenté en deux approches. L'approche déterministe et l'approche probabiliste.
-L'algorithme de **Cantor-Zassenhauss**, plus rapide que l'algorithme de **Elwin R. Berlekamp**.
Enfin, la décomposition sur des corps finis, de polynômes particuliers : Les polynômes cyclotomiques .

Chapitre 1

GENERALITES

1.1 Anneaux et corps

1.1.1 Anneaux

DEFINITION 1.1.1 (1)

1 . Un anneau est la donnée d'un triplet $(A, +, \times)$ où A est un ensemble muni deux lois de composition interne, notées $+$ et $\times$ vérifiant :
$(A, +)$ est un groupe abélien.

- *La loi $\times$ est associative et distributive par rapport à la loi $+$*
  c'est à dire : $\forall x, y, z \in A,\ x \times (y + z) = x \times y + x \times z$ et $(y + z) \times x = y \times x + z \times x$

2 . Soit $A' \subset A$ où $(A, +, \times)$ est un anneau
On dit que A' est un **sous − anneau** *de A si : $(A', +, \times)$ a une structure d'anneau.*

3 . L'anneau $(A, +, \times)$ est **commutatif** *si la loi $\times$ est commutatif.*

4 . L'anneau est dit **unitaire** *si la loi $\times$ admet un élément neutre.*

5 . L'anneau est dit **intègre** *s'il vérifie :*
$\forall x, y \in A$; $x \times y = 0 \Leftrightarrow x = 0$ ou $y = 0$. Sinon, ils existent $x, y \in A$ non nuls tel que $x \times y = 0$. dans cas x,y sont appelés **diviseurs de zéro**.

Exemple

$(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +, \times)$ est un anneau commutatif, unitaire et non nécessairement intègre.

PROPOSITION 1.1.1

Soit $(A, +\times)$ un anneau unitaire. L'ensemble des éléments inversibles (symétrisable), c'est à dire $A^* = \{x \in A : \exists y \in A : y \times x = x \times y = 1_A\}$, admet une structure de groupe .
Il est appelé le **groupe des unités de A** *s'il est muni de la multiplication et il est noté $\mathcal{U}(A)$ ou $A^\times$.*

PROPOSITION 1.1.2 (1)

1 . Toute intersection de sous-anneaux d'un anneau est un sous anneau de A.

2 . Tout sous-anneau d'anneau commutatif (respectivement intègre), est commutatif (respectivement intègre).

REMARQUE 1.1.1 *Une réunion de sous-anneaux n'est pas forcément un sous anneau.*

PROPOSITION 1.1.3

Soit $(A, +, \times)$ un anneau.
Soit $S \subset A$ non vide, alors le plus petit sous anneau de A contenant S existe et il est égal à l'intersection de tous les sous-anneaux de A contenant S, appelé **sous − anneau de A engendré par S**.

DEFINITION 1.1.2 *(Morphisme d'anneaux)*
Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux.
Un morphisme d'anneau *entre A et B est la donnée d'une application $f : A \longrightarrow B$ qui vérifie :*

1 . f est un morphisme de groupe pour la loi + : $f(x + y) = f(x) + f(y)$

2 . $f(x \times y) = f(x) \times f(y) \qquad \forall x, y \in A$.
Si f est bijective alors on dit que f est un **isomorphisme d'anneaux**.
On dit aussi qu'on a un isomorphisme d'anneaux unitaires si $f(1_A) = 1_B$.

1.1.2 Caractéristique d'un anneau

DEFINITION 1.1.3 *(caractéristique d'un anneau)*
Soit A un anneau. La caractéristique d'un anneau est notée car(A) et définie par $car(A) = inf\{n \in \mathbb{N}^* : n1_A = 0\}$, si cet ensemble est non vide, sinon $car(A) = 0$

On peut aussi définir la caractéristique d'un anneau de la manière suivante.
Il existe un unique morphisme d'anneaux de $\mathbb{Z}$ dans A définie par :

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow A \\ n &\longmapsto n.1_A \end{aligned}$$

kerf est un idéal de $\mathbb{Z}$ donc il existe un unique entier naturel p tel que $kerf = p\mathbb{Z}$, comme $f(1) = 1_A \neq 0$, p est distinct de $1_{\mathbb{Z}}$. L'entier ainsi définie s'appelle la **caractéristique de l'anneau** *on la note car(A) =p.*

REMARQUE 1.1.2

Si $p = 0$, alors $Kerf = \{0\}$ donc f est injective et $\mathbb{Z}$ est isomorphe à imf par conséquent A contient un sous-anneau isomorphe à $\mathbb{Z}$ et en particulier A est infini.

Si $p \neq 0$ alors $Kerf = p\mathbb{Z}$ et $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est isomorphe à imf. p est le plus petit entier positif tel que $p.1_A = 0$.
$p \in \mathbb{N}$ est caractérisé par : $\forall n \in \mathbb{N}\ n.1_A = 0 \Leftrightarrow$ n multiple de p.

PROPOSITION 1.1.4

Si l'anneau A est intègre sa caractéristique est soit 0 soit un nombre premier.

1.1.3 Idéaux d'un anneau

DEFINITION 1.1.4

Soit $(A,+,\times)$ un anneau et soit $I \subset A$.

1 . I est un idéal à gauche (respectivement à droite) de A si et seulement si : I est un sous-groupe abélien de A pour la loi (+) et $\forall a \in A$, $\forall x \in I$, $a \times x \in I$, $(x \times a \in I)$.

2 . I est un idéal bilatère si et seulement si I est un idéal à gauche et à droite

3 . I est un idéal propre ou strict si $I \neq A$.

4 .I un idéal est dit premier si et seulement si $\forall x, y \in A$, $x \times y \in I \implies x$ ou $y \in I$.

5 . Si I est un idéal bilatère. On dit que I est maximal s'il est strict et s'il n'est contenu dans aucun autre idéal que l'anneau tout entier.

REMARQUE 1.1.3 *Soit $(A,+,\times)$ un anneau unitaire. Soit I un idéal de A. Si I contient l'élément unité de A ou un élément inversible de A si et seulement si I= A.*

Dans un anneau, une intersection d'idéaux bilatères est un idéal bilatère.

DEFINITION 1.1.5

Soit $(A,+,\times)$ un anneau unitaire et soit I un idéal de A

1 .I est dit principal s'il est engendré par un seul élément (I est de la forme $I = sA$ ou As avec $s \in A$).

2 . I est dit de type fini s'il existe $S \subset A$ fini engendrant I.

PROPOSITION 1.1.5 *Soit $f : (A,+,\times) \longrightarrow (B,+,\times)$ un morphisme d'anneaux.*
On a $kerf = \{a \in A : f(a) = 0\}$ (c'est le noyau de f) et imf=f(A) (c'est l'image de f). Alors

- *kerf est un idéal de A*
- *imf est un sous anneau B*

Soit $f : A \longrightarrow B$ un morphisme d'anneau.

1 Si I est un idéal bilatère de B alors $f^{-1}(I)$ est un idéal bilatère de A

2 . Si I est un idéal premier de B alors $f^{-1}(I)$ est un idéal premier de A

REMARQUE 1.1.4 *Ceci n'est pas vrai pour un idéal maximal. Notons que : Un idéal I est dit premier $\Leftrightarrow \forall\ a, b \in A$ et $ab \in I \Rightarrow a \in I$ ou $a \in I$. Par contre I est dit maximal si et seulement si $I \subset J \subset A$ et J idéal $\Rightarrow I = J$ ou $J = A$.*

PROPOSITION 1.1.6 *Soit $(A,+,\times)$ un anneau et I un idéal bilatère .*
On considère la relation d'équivalence : $x\mathcal{R}y \Longleftrightarrow x - y \in I$.
L'ensemble des classes d équivalence noté $\dfrac{A}{\mathcal{R}}$ peut être muni d'une structure d'anneau de la façon suivante :

$$\overline{x} + \overline{y} = \overline{x + y}$$
$$\overline{x} \times \overline{y} = \overline{x \times y}$$

$\forall\ \overline{x}, \overline{y} \in \dfrac{A}{\mathcal{R}}$ *avec* $\overline{x} = x + I$

Cet anneau est appelé anneau quotient associé à I qu'on notera $\dfrac{A}{I}$.

REMARQUE 1.1.5 *soit A un anneau et I un idéal bilatère on a*

1 . A commutatif $\Longrightarrow \dfrac{A}{I}$ *est commutatif*

2 . A est unitaire $\Longrightarrow \dfrac{A}{I}$ *est unitaire*

En général beaucoup de propriétés ne passent pas au quotient.

1.1.4 Anneau euclidien

DEFINITION 1.1.6 *On dit qu'un anneau est* **euclidien** *s'il est intègre et s'il existe une application*
$\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$, *appelé* **stathme**, *telle que pour tous éléments a et b, avec* $b \neq 0$ *il existe des éléments q et r tels que l'on ait :*
$a = bq + r$ *et* $(r = 0,$ *ou* $\delta(r) < \delta(b))$ *et* $\delta(a) \leq \delta(ab)$ *une telle application est dite valuation euclidienne sur A*

1.1.5 Anneaux principaux

DEFINITION 1.1.7

On dit qu'un anneau est principal s'il est intègre et si tous ses idéaux sont principaux.

1.1.6 Anneaux factoriels

DEFINITION 1.1.8

Un élément $p \in A$ *est irréductible si et seulement :*

(i) $p \in A^*$ *où* A^* *est l'ensemble des éléments inversibles de A.*

(ii) $p = ab$ *implique que* $a \in A^*$ *ou* $b \in A^*$.

DEFINITION 1.1.9 *Un anneau A est factoriel si et seulement si :*

i) A est intègre.

ii) $\forall a \in A \setminus \{0\}$, *a s'écrit* $up_1p_2...p_r$ *avec* $u \in A^*$ *et* $p_1, p_2...p_r$ *irréductibles (propriété que lâ€™*^{TM} *on notera (E)).*

iii) La décomposition précédente est unique, aux inversibles près et à l'ordre près (propriété notée (U).

1.2 Corps

DEFINITION 1.2.1 *Un corps est la donné d'un triplet* $(K, +, \times)$ *tel que :*
- K n'est pas réduit à $\{0\}$
- $(K, +, \times)$ *est un anneau unitaire*
- Tout élément de $K \setminus \{0\}$ *est inversible par la loi* $\times$.
on dit que $(K, +, \times)$ *est un corps commutatif si la loi* $\times$ *est de plus commutative*

REMARQUE 1.2.1 (1))

1) Si $n \geq 2$, $(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +, \times)$ *est un corps* $\Leftrightarrow$ *n est premier.*

2) Soit $(K, +, \times)$ *un corps, on a alors* $(K, +, \times)$ *est un anneau intègre et* $1 \neq 0$

3) Tout anneau intègre, fini et non réduit à $\{0\}$ *est un corps.*

4) Soit A un anneau alors A est un corps si et seulement si ses seuls idéaux sont $\{0\}$ *et A.*

5) Soit $f : K \longrightarrow A$ *un morphisme d'anneau ou K est un corps et A un anneau non réduit à* $\{0\}$. *On a alors :*

- f est injectif où nul

- Si, de plus A est un corps et $f \neq 0$ *alors f est dit morphisme de corps.*

1.2.1 Sous corps d'un corps

DEFINITION 1.2.2 *Soit K un corps, soit P une partie de K. les assertions suivantes sont équivalentes .*

1) P est non vide, et une partie stable (pour les lois $+, \times$) de K et P muni des lois induites par celle de K est lui-même un corps.

2) P est un sous-anneau de K, $1 \in P$ et $(x \in P \Rightarrow x^{-1} \in P)$.

3) P est un sous groupe de $(K, +)$ et $P^\star = P\backslash\{0\}$ est un sous groupe du groupe multiplicatif $(K^\star, \times)$, on dit que P est ***un sous-corps de*** *K.*

Exemple

– - $\mathbb{Q}$ est un sous corps de $\mathbb{R}$
  - $\mathbb{R}$ est un sous corps de $\mathbb{C}$

REMARQUE 1.2.2

Soit K un corps. Toute intersection de sous -corps de K est un sous - corps de K.

1.2.2 Caractéristique d'un corps

PROPOSITION 1.2.1

Soit K un corps alors on a :

1) $carac(K) = 0$ ou un nombre premier p

2) Soit L un corps tel que $f : K \longrightarrow L$ est un morphisme de corps non nul alors : $carac(K) = carac(L)$

DEFINITION 1.2.3 *Un corps K est dit premier s'il est isomorphe à $\mathbb{Q}$ où à l'un des corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$ avec p un nombre premier.*

1.3 Quelques résultats fondamentaux

THEOREME 1.3.1 *(Lagrange)*
Soit (G,.) un groupe fini de cardinal n
Soit H un sous-groupe de G d'ordre k. Alors k divise n.
En particulier : L'ordre de tout élément de G divise l'ordre de G.

Preuve

Soit $\mathcal{R}$ la relation d'équivalence à gauche modulo H.
Les classes d'équivalences pour $\mathcal{R}$ forment une partition de G. Soient $x_1H, \cdots x_lH$ toutes les classes pour $\mathcal{R}$, deux à deux distinctes.
Donc $card(G) = Card(x_1H) + Card(x_2H) \cdots + Card(x_lH)$
Or $Card(x_iH) = Card(H)$ Donc $Card(G) = \underbrace{Card(H) + \cdots + Card(H)}_{lfois}$ Donc $n = lk$ donc k divise n et $q = \frac{n}{k}$ nombres de classes pour $\mathcal{R}$.

THEOREME 1.3.2 *(équation aux classes)*
Soit G un groupe fini noté multiplicativement et considrons l'action de conjugaison de G sur G, donnée par $x.g = x^{-1}gx$.
$Z(G)$ le centre de G tel que $Z(G) = \{x \in G : \forall y \in G, xy = yx\}$.
Ω l'ensemble des classes de conjugaisons non réduites à un singleton.
Et, pour chaque $x \in G$, $S_x = \{g \in G : g^{-1}xg = x\}$ le stabilisateur de x. Alors
$|G| = |Z(G)| + \sum_{C \in \Omega} \frac{|G|}{|S_x|}$ *(somme dans la laquelle on prend un et un seul élément x dans chacune des classes C de Ω).*

LEMME 1.3.1 *(Théorème des restes chinois pour les anneaux polynomiaux)*
Soient $\mathbb{K}$ un corps commutatif et $P_1(X), \cdots, P_n(X)$ n polynômes de $\mathbb{K}[X]$ deux à deux premiers entre eux. Si $(P_i(X))$ désigne l'idéal engendré par $P_i(X)$, Alors $\frac{\mathbb{K}[X]}{(P_1(X)\cdots P_n(X))}$ et $\frac{\mathbb{K}[X]}{(P_1(X))} \times \cdots \times \frac{\mathbb{K}[X]}{(P_n(X))}$ sont isomorphes en tant qu'anneaux.

1.4 Les extensions de corps

DEFINITION 1.4.1

*On appelle **extension d'un corps** k, tout corps L qui contient une image de k par un homomorphisme d'anneau non nul (nécessairement injectif) :*

$$\varphi : k \hookrightarrow L$$

On peut alors dire qu'une extension d'un corps k est un corps K qui contient un sous corps isomorphe à k. On note $K \mid k$, si K est une extension de k.

REMARQUE 1.4.1 (1)

1 . Si $k \subset L$, alors on dit que L est une extension de k.

2 . Si L est une extension de k, il est muni ipso facto d'une structure de k-espace vectoriel : $\forall \alpha \in k$, $\forall x \in L$, on pose : $\alpha x = \varphi(\alpha).x$.

Exemple

- $\mathbb{R}$ est une extension de $\mathbb{Q}$.
- $\mathbb{C}$ est une extension de $\mathbb{R}$.

1.4.1 éléments algébriques et éléments transcendants sur un corps donné

Soit k un corps commutatif, L une extension de k.

Un élément $\xi \in L$ est dit algébrique sur k si le k-homomorphisme de substitution

$$\begin{aligned} \varphi_\xi : k[X] &\longrightarrow L \\ P(X) &\longmapsto P(\xi) \end{aligned}$$

n'est pas injectif.
ξ est dit transcendant sur k si φ_ξ est injectif

On peut dire simplement qu'un élément $\xi \in L$ est algébrique sur k s'il existe un polynôme non nul $P \in k[X]$ tel que $P(\xi) = 0$.

Si $\xi \in L$ est un élément algébrique sur k, on appelle polynôme minimal de ξ sur k l'unique polynôme normalisé $f_\xi(X) \in k[X]$ tel que

$$ker\varphi_\xi = f_\xi[X]k[X]$$

Le degré de f_ξ est appelé degré de ξ sur k.
Notation L'image de φ_ξ est notée $k[\xi]$ et $k[\xi]$ est le corps de fraction de $k[\xi]$.

THEOREME 1.4.1

Soit L une extension de k. Les trois assertions suivantes sont équivalentes :

i) ξ est algébrique sur k.

ii) $k[\xi] = k(\xi)$.

iii) $k[\xi]$ est un k-espace vectoriel de dimension finie.

Preuve

i) $\Longrightarrow$ *ii)* On a $k[\xi] \subset k(\xi)$. Le corps $k(\xi)$ est le sous-corps de L constitué des éléments $P(\xi)/Q(\xi)$ avec P,Q $\in k[X]$ et $Q(\xi) \neq 0$. Soit M_ξ le polynôme minimal de ξ. Les polynômes M_ξ et Q sont premiers entre eux, donc d après Bezout, il existe U,$V \in k[X]$ tel que $UM_\xi + VQ = 1$ et par suite $1/Q(\xi) = V(\xi) \in k[\xi]$ et donc $P(\xi)/Q(\xi) \in k[\xi]$ c'est à dire $k(\xi) \subset k[\xi]$.

ii) $\Longrightarrow$ *i)* Il existe un entier n et des éléments non tous nul $a_o, \cdots, a_n$ de k tel que $\xi^{-1} = a_0 + \cdots + a_n\xi^n$. On a donc

$$a_n\xi^{n+1} + \cdots + a_0\xi - 1 = 0$$

ce qui prouve que ξ est algébrique sur k.
ii) $\Longrightarrow$ *iii)* On sait que ($i \Leftrightarrow ii$) ξ est algébrique, donc que $dim_k k[\xi] < +\infty$. On a donc $k[\xi]$ est un k-espace vectoriel de dimension finie.

iii) $\Longrightarrow$ *i)* Comme $k[\xi]$ est un $k-espace$ vectoriel dedimension finie, on a donc $dim_k k[\xi] = n < +\infty$ et par suite, ξ est algébrique sur k car la famille {1, ξ, ...,ξ^{n+1}} qui a plus que n éléments est liée.

1.4.2 Corps de rupture d'un polynôme

PROPOSITION 1.4.1

Soit k un corps commutatif et P(X) un polynôme irréductible sur k. Alors
il existe une extension de L de k, degré $[L : k] = deg(P)$, dans laquelle $P(X)$ admet au moins une racine u.
Ce corps est la plus petite extension de k (en terme de degré) qui contient la racine u.

Preuve

On a P(X) qui est un polynôme irréductible sur $k[X]$ donc $\frac{k[X]}{(P(X))}$ est un corps.
Considérons le morphisme suivant :

$$\begin{aligned} \pi : k &\longrightarrow \frac{k[X]}{(P(X))} \\ a &\longmapsto \overline{a} \end{aligned}$$

C'est une injection de k dans L, où $L = \frac{k[X]}{(P(X))}$.

Ainsi L est une extension de k
Posons $u = \overline{X} = X + (P(X))$, on a $P(\overline{X}) = \sum_{i=0}^{n} a_i\overline{X^i} = \overline{\sum_{i=0}^{n} a_iX^i} = \overline{P(X)}$

or $P(X) \in (P(X))$ donc $\overline{P(X)} = \overline{0}$ alors $P(u) = 0$
Comme $L = k[\overline{X}] = k[u]$, alors L est bien une plus petite extension de k contenant u.

DEFINITION 1.4.2

Soit k un corps commutatif et soit $P(X)$ un polynôme irréductible sur k. Le corps $\frac{k[X]}{(P(X))}$, est un **corps de rupture du polynôme** $P(X)$.

Exemple

Pour $k = \mathbb{Q}$:
(i) Un corps de rupture de $P(X) = X^2 + X + 1$ est $\mathbb{Q}[j]$ avec $j = e^{\frac{2i\pi}{3}}$
(ii) Un corps de rupture de $Q(X) = X^3 - 2$ est $\mathbb{Q}[\sqrt[3]{2}]$.

DEFINITION 1.4.3

Soit k un corps commutatif et soit P(X) un polynôme dans k[X]. On dit que P est scindé sur k si P est produit de polynômes de degré 1 dans k[X].

PROPOSITION 1.4.2

Soit k un corps commutatif et soit P(X) irréductible de degré d sur k. Il existe une extension L de k dans laquelle P(X) est scindé.

Preuve

soit L_1 un corps de rupture de P(X) et soit $u_1 \in L_1$ une racine de p(X). Alors $P(X) = (X - u_1)P_1(X)$ avec $P_1(X) \in L_1[X]$. Il est clair que $L_1 = k[u_1]$.
1er cas : si $P_1(X)$ est irréductible sur L_1, on considère $L_2 \supset L_1$ un corps de rupture de $P_1(X)$ et si $u_2 \in L_2$ est une racine de P_1. alors $P_1(X) = (X-u_2)P_2(X)$ avec $P_2(X) \in L_2[X]$. Alors $L_2 = k[u_1, u_2]$ et contient 2 racines de $P(X)$. Si l'argument précedent tient on continue le processus et il existe une extension $L_d = k[u_1, \cdots, u_d]$ et les éléments $u_1 \cdots u_d$ tels que $P(X) = (X - u_1) \cdots (X - u_d)$.
2 ème cas : si $P_1(X)$ est réductible sur L_1 on considère les composantes irréductibles de $P_1(X)$ et on continue comme dans le premier cas jusqu'à épuisementde chacune d'elles. En définitive on arrive à la mêmeconclusion que dans le cas 1.

PROPOSITION 1.4.3

Soit k un corps commutatif et soit P(X) un polynôme non constant sur k. Alors il existe une extension L de k dans laquelle P(X) est scindé.

Preuve

Si degP(X) = 1, $P(X)$ est scindé dans $k[X]$, donc $L = k$.
Si $degP \geq 2$, on fait alors une récurrence sur le degré de $P(X)$, on distingue le cas où $P(X)$ est irréductible sur k, on fait alors intervenir un corps de rupture de $P(X)$ dans lequel $P(X) = (X - u_1)P_1(X)$ avec $P_1(X) \in L_1[X]$ et $\deg(P_1(X)) < \deg(P(X))$, mais alors par hypothèse de récurrence $P_1(X)$ est scindé dans une extension L' de L' et en définitive $P(X)$ est scindée dansl'extension de k donnée par $L = L_1L'$.
Si $P(X)$ est réductible sur k, on applique le raisonemment précédent au à une de ses composante irréductible.

1.4.3 Corps de décomposition d'un polynôme

DEFINITION 1.4.4

Soit k un corps commutatif et soit P(X) un polynôme non constant dans $k[X]$.
On appelle ***corps de décomposition ou de racines*** *de $P(X)$ sur k toute extension L de k dans laquelle $P(X)$ est scindé et L est engendré (comme corps ou comme anneau) par les racines de P(X)sur L.*
Ainsi un corps de décomposition est une extension minimale de k sur laquelle $P(X)$ est scindé.

COROLLAIRE 1.4.1

Soit $P(X)$ tel que $degP = d$, L est un corps de décomposition de P si et seulement si
(i) Il existe $u_1, \cdots u_d \in L$ tels que $P(X) = (X - u_1) \cdots (X - u_d)$.
(ii) Si L' est une extension de k telle que P y soit scindé, alors L' est une extension de L.

Exemple

soit $k = \mathbb{Q}$
Le corps $L = \mathbb{Q}[\sqrt[3]{2}, j]$ est le corps de décomposition de $P(X) = X^3 - 2$.
Notons que $j = e^{\frac{2i\pi}{3}}$

DEFINITION 1.4.5

(i) Un corps k est algébriquement clos si tout polynôme dans k[X] est scindé sur k
(ii) On appelle clôture algébrique d'un corps k tout corps algébriquement clos qui est une extension algébrique de k que l'on note $\overline{k}$.

1.4.4 Extension normale et séparable

DEFINITION 1.4.6

i) Une extension L d'un corps k est dite normale si tout polynôme irréductible dans $k[X]$ qui admet une racine dans L est scindé sur L.

ii) Un polynôme irréductible dans k[X] est séparable sur k s'il n'admet que des racines simples dans son corps de décomposition. Dans le cas contraire on dit le polynôme est inséparable.

iii) Un polynôme est séparable si toutes ses composantes irréductibles sont séparables.

iv) Un élément algébrique sur k est dit séparable si son polynôme minimal est séparable.

v) une extension algébrique L de k est dite séparable si tout élément de L est séparable.

REMARQUE 1.4.2

En règle générale il est difficile de produire une extension non séparale.

PROPOSITION 1.4.4 *Soit k un corps commutatif. Une extension L de k est normale finie si et seulement si L est le corps de décomposition d'un polynôme non constant dans $k[X]$.*

Preuve

$\Longrightarrow$) soit L est une extension de k normale finie
Comme L est finie, alors il existe $u_1 \cdots u_d \in L$ tels que $L = k[u_1 \cdots u_d]$. On note $\mathcal{M}_i(X)$ le polynôme minimal de u_i. Soit $P(X) = \mathcal{M}_1(X) \cdots \mathcal{M}_d(X)$. Comme $\mathcal{M}_i(X)$ est irréductible dans $k[X]$ et admet une racine u_i dans L alors il est scindé sur L . Et par conséquent, L contient toutes les racines de $P(X)$, donc L est le corps de décomposition de P.
$\Longleftarrow$) Supposons que L soit le corps de décomposition d'un polynôme $P(X)$ avec $deg(P(X)) = d$ alors $[L : k] \leq d!$

Soit $Q(X)$ un polynôme irréductible dans $k[X]$ ayant une racine u dans L.
on considère L' le corps de décomposition de $P(X)Q(X)$. Soit v une racine de $Q(X)$ dans L'.

On a les inclusions suivantes et les relations entre leurs degrés :

$$k \hookrightarrow k[u] \hookrightarrow L[u] \hookrightarrow L'$$

et

$$k \hookrightarrow L \hookrightarrow L[u] \hookrightarrow L'$$

avec $[L(u) : k] = [L(u) : k(u)][k(u) : k] = [L(u) : L][L : k]$

$$k \hookrightarrow k[v] \hookrightarrow L[v] \hookrightarrow L'$$

et

$$k \hookrightarrow L \hookrightarrow L[v] \hookrightarrow L'$$

avec $[L(v) : k] = [L(v) : k(v)][k(v) : k] = [L(v) : L][L : k]$.

comme u et v sont des racines du même polynôme irréductible sur k, alors $[k(u) : k] = [k(v) : k] = degQ$.
D un autre coté, comme $L[u]$ est un corps de décomposition de $P(X)$ sur $k[u]$ et $L[v]$ est le corps de décomposition de $P(X)$ sur $k[v] \cong k[u]$ et par unicité du corps de décomposition, on a $[L[u] : k[u]] = [L[v] : k[v]]$ et ainsi, $[L[u] : k] = [L[v] : k]$ d'ou $1 = [L[u] : L] = [L[v] : L]$ et par conséquent $v \in L$.

PROPOSITION 1.4.5

Soit un k corps commutatif. Alors si $P(X) \in k[X]$ est irréductible tel que P' (le polynôme dérivé) soit non nul, alors P est séparable.

Preuve

Comme P est irréductible dans k[X], alors il est premier avec son polynôme dérivé P'. Ainsi par Bezout, il existe U,V tels que $UP + VP' = 1$. Cette relation étant aussi vraie dans le corps de décomposition, alors ils sont premiers dans ce corps également.
si P admet une racine double dans son corps de décomposition alors cette racine est aussi racine du polynôme dérivé P' non nul. Ce qui est absurde.

PROPOSITION 1.4.6

Soit k un corps de caractéristique p.
Un polynôme irréductible $P(X)$ est inséparable sur k si et seulement si il existe un polynôme $Q(X) \in k[X]$ tel que $P(X) = Q(X^p)$.

Preuve

Si P est irréductible dans $k[X]$, alors on a :
(i) Soit P' est non nul et il est premier avec son polynôme dérivé P' et ainsi, P est séparable.
(ii) Soit P' est nul. si $P(x) = a_0 + a_1X + \cdots + a_dX^d$, on a $P'(X) = a_1 + 2a_2X + \cdots da_dX^{d-1} = 0$ ainsi, $ka_k = 0$ et par conséquent

$$P(X) = \sum_{j=0}^{d} a_{jp}X^{jp}$$

et par conséquent il existe un polynôme $Q(X) \in k[X]$ tel que $P(X) = Q(X^p)$.
Réciproquement, s il existe un polynôme $Q(X) \in k[X]$ tel que $P(X) = Q(X^p)$, alors $P' = 0$ et ainsi, $pgcd(P, P') = P$ donc P est inséparable.

Chapitre 2

Fonctions arithmétiques

2.1 Fonctions multiplicatives

DEFINITION 2.1.1 (1))

1) 1. *On appelle fonction arithmétique, toute fonction définie sur* $\mathbb{N}^*$ *et à valeurs dans* $\mathbb{R}$ *ou* $\mathbb{C}$. *Le nombre* $f(n)$ *est définis à partir des propriétés arithmétiques de l'entier* n.

2) *Une fonction arithmétique est dite multiplicative si elle vérifie les conditions suivantes :* $f(1) = 1$ *et* $f(mn) = f(m)f(n)$,$\forall m, n \in \mathbb{N}^* / (m, n) = 1$.
Ainsi une fonction arithmétique sera entièrement déterminée par les valeurs qu'elle prend sur les puissances p^α *des nombres premiers.*

3) *Si de plus, la propriété* $f(mn) = f(m)f(n)$ *est vérifiée pour tous les couples d'entiers, on dit que* f *est complètement multiplicative.*

4) *on peut aussi définir des fonctions arithmétiques additives, à savoir :* $f(1) = 0$ *et* $f(mn) = f(m) + f(n)$, *pour tout couple d'entiers* m *et* n *premiers entre eux. (La fonction ln en est un exemple).*
Dans tous les cas : f *est alors déterminée par sa restriction à l'ensemble* $\mathcal{P}$ *des nombres premiers (dans des fonctions totalement multiplicatives ou totalement additives).*

PROPOSITION 2.1.1 *Soit* f *une fonction multiplicative et* F *la fonction arithmétique définie par*

$$F(n) = \sum_{d|n} f(d)$$

Alors F*est multiplicative (c'est la somme de Dirichlet).*

DEFINITION 2.1.2

On appelle fonction de Möbius, la fonction arithmétique μ, *définie dans l'ensemble des entiers naturels non nuls, et à valeurs sur* $\{-1, 0, 1\}$, *telle que :*

1. $\mu(1) = 1$
2. $\mu(n) = \begin{cases} (-1)^r \text{ si } n = p_1 \cdots p_r \text{ n'est divisible par le carré d'aucun nombre premier} \\ 0 \text{ si } n \text{ n'est pas de la forme } n = d^2k \end{cases}$

PROPOSITION 2.1.2

La fonction μ *de Möbius est multiplicative et vérifie :*

$$\mathrm{e}(n) = \sum_{d|m} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n > 1 \end{cases}$$

2.2 Structure de $\mathbb{C}$-algèbre de l'ensemble des fonctions arithmétiques

PROPOSITION 2.2.1

L'ensemble $\mathcal{A}$ des fonctions arithmétiques est muni d'une structure de $\mathbb{C}$-algèbre si l'on définit l'addition et la multiplication de la manière habituelle et si l'on prend pour produit $f*g$ de deux fonctions, le produit de convolution (ou produit) de Dirichlet défini par :

$$(f*g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{dd'=n} f(d).f(d')$$

***A** est dans une $\mathbb{C}$-algèbre associative, commutative et unitaire.*

THEOREME 2.2.1

Pour tout $f \in \mathcal{A}$, les conditions suivantes sont équivalentes :

(i) $f(1) \neq 0$.

(ii) $f \in \mathcal{U}(\mathcal{A})$ *(i.e* $\exists\, !\, g \in \mathcal{A}$ *tel que* $f*g = g*f = e$*).*

PROPOSITION 2.2.2 *(i)* $(f \in \mathcal{A}$ *et* $g = f*I) \Rightarrow f = g*\mu$

(ii) $(g \in \mathcal{A}$ *et* $f = g*\mu) \Rightarrow g = f*I$*. (I est l'inverse de la fonction de möbius)*

PROPOSITION 2.2.3 *Formule d'inversion de Möbius. Soient f et g deux fonctions arithmétiques, on a l'équivalence suivante :*

$$f(n) = \sum_{d|n} g(d) \Longleftrightarrow g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$$

REMARQUE 2.2.1

D'où l'on déduit la forme multiplicative de ce théorème :

$$f(n) = \prod_{d|n} g(d) \Longleftrightarrow g(n) = \prod_{d|n} f(\frac{n}{d})^{\mu(d)}$$

2.3 Cas de la fonction d'Euler

DEFINITION 2.3.1 *Soit $n \geq 1$ un entier naturel. On désigne par :*
$\varphi(n) = \#\{q\,;\,(q,n) = 1$ *et* $1 \leq q \leq n\}$
La fonction $\varphi(n)$ est appelée fonction (ou indicateur) d'Euler.

PROPOSITION 2.3.1

$\forall n \in \mathbb{N}^*$, *on a :*

$$\sum_{d|n} \varphi(d) = n.$$

Pour chaque $n \in \mathbb{N}$, nous avons

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n} \mu(d)\frac{\mu(d)}{d}.$$

La fonction d'Euler φ est multiplicative. Et pour $n > 1$, et $n = p_1^{\alpha_1}.p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, on a

$$\varphi(n) = n\prod_{j=1}^{r}(1 - \frac{1}{p_j}) = \prod_{j=1}^{r}(p_j - 1)p_j^{\alpha_j - 1}$$

où le produit est étendu aux diviseurs de n.

Chapitre 3

Corps fini

DEFINITION 3.0.2

Un corps fini est un corps dont le cardinal est fini

Exemple

Pour tout nombre premier p, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps fini

LEMME 3.0.1

Si L est un corps fini, alors :

- *L est de caractéristique p, où p est un nombre premier.*
- *L est de degré fini sur son sous-corps premier (isomorphe à $\frac{\mathbb{Z}}{p\mathbb{Z}}$) de L.*
- *Il existe $n \in \mathbb{N}^\star$ tel que $\mid L \mid = p^n$*

Preuve

Comme L est fini, alors L n'est pas une extension d'un corps isomorphe à $\mathbb{Q}$ et par conséquent il existe un nombre premier p tel que L soit une extension de son sous-corps premier noté $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$

Comme L est fini, alors L est un $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$-espace vectoriel de dimension finie d'oú il existe $n \in \mathbb{N}^*$ tel que L soit isomorphe à $(\dfrac{\mathbb{Z}}{p\mathbb{Z}})^n$, en tant qu'espace vectoriel et par conséquent $\mid L \mid = p^n$.

Lorsque q est une puissance d'un nombre premier ($q > 1$), nous allons montrer qu'il existe, à un isomorphisme près, un unique corps de cardinal q.

3.0.1 Existence et unicité des corps finis

THEOREME 3.0.1

Soit p un nombre premier et n un entier supérieur ou égal à 1, posons $q = p^n$.
Si Ω est un corps algébriquement clos de caractéristique p (qu'on peut prendre comme étant la clôture algébrique de $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$) il existe alors un sous corps de Ω et un seul qui soit de cardinal q, ce sous-corps est noté $\mathbb{F}_q$. En d'autre terme, c'est l'ensemble des racines du polynôme $X^q - X$.
De plus, tout corps fini de cardinal q est isomorphe à $\mathbb{F}_q$.

Le lemme suivant nous sera utile pour la preuve.

LEMME 3.0.2

Soit F un corps de caractéristique p l'application $\sigma_p : F \longrightarrow F$ tel que $\sigma_p(x) = x^p$ pour tout $x \in F$ est un homomorphisme de corps, cet homomorphisme est appelé homomorphisme de **Frobenius**.

Preuve

on a $\sigma_p(1_F) = 1_F^p = 1_F$

soient x,y $\in F$

$$\begin{aligned}\sigma_p(xy) &= (xy)^p \\ &= x^p y^p \\ &= \sigma_p(x)\sigma_p(y)\end{aligned}$$

soient x,y $\in F$

$$\begin{aligned}\sigma_p(x+y) &= (x+y)^p \\ &= x^p + \sum_{k=1}^{p-1} C_p^k x^p y^{p-k} + y^p\end{aligned}$$

Montrons que la quantité $\sum_{k=1}^{p-1} C_p^k x^p y^{p-k}$ est nulle
$C_p^k = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{k!} \Longrightarrow k!C_p^k = p(p-1)\cdots(p-k+1)$ donc $p \mid k!C_p^k$, comme $1 \leq k \leq p-1$ alors $p \wedge k = 1$ donc $p \wedge k! = 1$ d'après Gauss $p \mid C_p^k$, $C_p^k = lp = l(p.1_F) = 0$ avec $l \in \mathbb{Z}$ conséquent la quantité $\sum_{k=1}^{p-1} C_p^k x^p y^{p-k}$ est nulle.
Finalement $\sigma_p(x+y) = x^p + y^p$ ce qui montre que σ est un morphisme de corps.

Preuve du Théorème

Notons σ_q l'endomorphisme de Ω, puissance $q - ième$ de l'endomorphisme σ_p. Ainsi, si $x \in F$, $\sigma_q(x) = x^q$.
considérons l'ensemble des $x \in \Omega$ tels que $\sigma_q(x) = x$. C'est un sous corps de Ω.
Notons le $\mathbb{F}_q = \{x \in \Omega \ : \ \sigma_q(x) = x\}$.
C'est bien un corps, en effet : $\mathbb{F}_q \subset \Omega$. $1_\Omega \in \mathbb{F}_q$ car $\sigma(1_\Omega) = 1_\Omega$.
Soient x, $y \in \mathbb{F}_q$ on a : $\sigma_q(xy) = (xy)^q = x^q y^q = xy$.
Alors :

$$xy \in \mathbb{F}_q.$$

Soit $x \in \mathbb{F}_q$ on a : $\sigma(x^{-1}) = (x^{-1})^q = (x^q)^{-1} = x^{-1}$.
Alors :

$$x^{-1} \in \mathbb{F}_q$$

Soient x, $y \in \mathbb{F}_q$, on a :

$$\begin{aligned}\sigma_q(x+y) &= (x+y)^q \\ &= (x+y)^{p^n}\end{aligned}$$

Montrons que $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ pour tout entier naturel.
Raisonnons par récurrence
pour $n = 0$ l'énoncé est vrai, pour $n = 1$ on a $(x+y)^p = x^p + y^p$ d'après le lemme précédant. supposons que l'énoncé est vrai pour tout entier k tel que $0 \leq k \leq n$, c'est

à dire $(x+y)^{p^k} = x^{p^k} + y^{p^k}$ pour tout k tel que $0 \leq k \leq n$
Montrons que l'énoncé est vérifié au rang $n+1$ on a

$$\begin{aligned}(x+y)^{p^{n+1}} &= ((x+y)^{p^n})^p \\ &= ((x^{p^n} + y^{p^n}))^p \\ &= x^{p^{n+1}} + y^{p^{n+1}}\end{aligned}$$

Alors pour tout entier naturel on a : $(x+y)^{p^n} = x^{p^n} + y^{p^n}$
Donc $\sigma_q(x+y) = x^q + y^q$ comme $x, y \in F_q$, $\sigma_q(x+y) = x+y$ alors $x+y \in \mathbb{F}_q$
par conséquent, $\mathbb{F}_q$ est un sous corps de Ω.
La dérivée du polynôme $X^q - X$ est $qX^{q-1} - 1 = -1 \implies pgcd(X^q - X, -1) = 1$.
Puisque Ω est de caractéristique p et q est d'une puissance de p, ainsi le $X^q - X$ n'a pas de racine double et $\mathbb{F}_q$ est de cardinal q.

Réciproquement, si K est un sous corps de cardinal q de Ω. Tout élément $x \in K^*$ vérifie $x^{q-1} = 1$ (c'est le théorème de Lagrange, l'ordre d'un élément divise l'ordre du groupe) donc $x^q = x$ et $x \in F_q$ si bien que $K \subset \mathbb{F}_q$ comme les deux corps ont le même cardinal, $K = F_q$ ce qui montre l'unicité.
Soit enfin K un corps fini de cardinal q alors K est une extension algébrique finie de $\mathbb{F}_p$. Comme Ω est une extension algébrique close du corps $\mathbb{F}_p$, il existe un homomorphisme de corps $i : K \longrightarrow \Omega$. alors $i(K)$ est un corps de cardinal q contenu dans Ω donc $i(K) = \mathbb{F}_q$ et $K \simeq \mathbb{F}_q$.

3.0.2 Groupe multiplicatif d' un corps fini

THEOREME 3.0.2

Soit K un corps et G un sous groupe fini du groupe multiplicatif de K, G est un groupe cyclique. En particulier, le groupe multiplicatif d'un corps fini est cyclique.

Preuve

Soit G un groupe abélien fini, notons n le cardinal de G.
D'après le théorème des facteurs invariants il existe des entiers $d_1 \mid d_2 \mid \cdots \mid d_r$, avec $d_1 > 1$, tels que $G \simeq \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_r\mathbb{Z}}$ et $n = d_1 \cdots d_r$
En particulier tout élément de G est annulé par d_r autrement dit, tout élément x de G vérifie $x^{d_r} = 1$ ie les n éléments de G vérifient l'équation.
Cependant, un polynôme à coefficient dans un corps (commutatif) a moins de racines que son degré (sauf si c'est le polynôme nul).
Ainsi $d_r \geq n = d_1 \cdots d_r$ on a donc $r = 1$, $d_1 = n$ et $G \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$ est cyclique d'ordre n.

COROLLAIRE 3.0.1

Soit K un corps fini de cardinal q. Le groupe K^* possède exactement $\varphi(q-1)$ générateurs, ou φ est l'indicateur d'Euler. De plus, si α est un générateur de K^*, l'ensemble des générateurs de K^* est :
$\{\alpha^k : 1 \leq k \leq q-1 : pgcd(k, q-1) = 1\}$.

Exemple

Considérons le polynôme $F[X] = X^3 + X + 1 \in \mathbb{F}_5[X]$. Posons $K = \mathbb{F}_5[X]/(F[X])$.

Le polynôme F est irréductible sur $\mathbb{F}_5$, car il est de degré 3 et n'a pas de racines dans $\mathbb{F}_5$, donc K est un corps, et c'est aussi un $\mathbb{F}_5$ -EV de dimension 3. Sa caractéristique est 5 et son cardinal est $5^3 = 125$. Le groupe K^* est donc cyclique d'ordre 124. Les ordres possibles de ses éléments sont : 1,2,4,31,62 et 124. Il possède $\varphi(125-1) = 60$ générateurs.

Soit α la classe $X \mod (F)$ Le système $(1, \alpha, \alpha^2)$ est une base de K sur $\mathbb{F}_5$.

Vérifions que 2α est un générateur de K^*, c'est à dire d'ordre124. On a

$$\alpha^3 = -1 - \alpha, \alpha^5 = 1 + \alpha - \alpha^2$$

Puisque la caractéristique est 5, il en résulte que l'on a

$$\alpha^{15} = -(1+\alpha)^5 = -1 - \alpha^5 = \alpha^2 - \alpha - 2,$$

d'oú les égalités

$$\alpha^{30} = \alpha^2 + 1, \alpha^{31} = -1$$

Ainsi, α est d'ordre 62. par ailleurs, on a $2^4 \equiv 1 \mod 5$ et $2^{31} \equiv 3 \mod 5$ d'oú $(2\alpha)^{31} = 2$ et $(2\alpha)^{62} = -1$, ce qui entraine notre assertion.

3.0.3 Corps finis comme quotient

COROLLAIRE 3.0.2

Soit K un corps fini de cardinal p^n. Il existe un polynôme $F \in \mathbb{F}_p[X]$ de degré n irréductible sur $\mathbb{F}_p$, tel que K et $\mathbb{F}_p[X]/(F)$ soient isomorphes.

Preuve

Soit α un générateur de K^*. Considérons l'application

$$\psi : \mathbb{F}_p[X] \longrightarrow K$$

définie pour tout $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{F}_p[X]$ par l'égalité

$$\psi(P) = \sum_{i=0}^{n} a_i \alpha^i,$$

où l'on identifie ici $a_i \in \mathbb{F}_p$ avec n'importe quel entier relatif dont la classe modulo p est a_i. Cela est licite car K est de caractéristique p. Notre application ainsi définie est un morphisme d'anneau. Il est surjectif car α est une générateur de K^*. Le noyau de ce morphisme est un idéal non nul I de $\mathbb{F}_p[X]$ et $\mathbb{F}_p[X]/I$ est un anneau isomorphe à K. Il existe $F \in \mathbb{F}_p[X]$ non nul tel que $I = (F)$ car $\mathbb{F}_p[X]$ est un anneau principal. Puisque $\mathbb{F}_p[X]/(F)$ est un corps car isomorphe à K, F est irréductible sur $\mathbb{F}_p$. Si m est le degré de F, le cardinal de $\mathbb{F}_p[X]/(F)$ est p^m. C'est aussi le cardinal de K, d'où $m = n$.

REMARQUE 3.0.1

Un défaut de la démonstration précédente est qu'elle ne fournit pas de moyen effectif de déterminer un corps fini. D'après le corollaire, on sait toutefois qu'il nous faut un polynôme irréductible de degré convenable. Après avoir montré l'existence et l'unicité de $\mathbb{F}_q$ il est assez naturel de se demander quels sont les sous-corps de $\mathbb{F}_q$? La réponse découle essentiellement du lemme préliminaire suivant.

3.0.4 Sous corps d'un corps fini

LEMME 3.0.3

Soit a un entier supérieur à 2, d et n deux entiers naturels.

$$a^d - 1 | a^n - 1 \Longleftrightarrow d | n$$

.

Preuve

. Supposons que $d|n$ alors il existe $b \in \mathbb{Z}^*$ tel que $n = bd$. Alors :
$a^n - 1 = a^{bd} - 1 = (a^d)^b - 1 = (a^d - 1)((a^d)^{b-1} + \cdots + 1)$
Posons $N = (a^d)^{b-1} + \cdots + 1$ On a :$a^n - 1 = (a^d - 1)N$.
Par conséquent $a^d - 1|a^n - 1$.
Réciproquement supposons que $a^d - 1|a^n - 1$.
écrivons la division euclidienne de n par d : $n = bd + r$ avec $0 \leq r < d$.

. Raisonnons par l'absurde en supposant que r soit non nul
Modulo $(a^d - 1)$, on a $a^d \equiv 1(\mod a^d - 1)$. donc $a^{bd} \equiv 1(\mod a^d - 1)$. Or par hypothèse $a^n - 1 \equiv 0(\mod a^d - 1)$ donc $a^n \equiv 1(\mod a^d - 1)$ donc : $a^{bd} \times a^r \equiv a^r(\mod a^d - 1) \equiv 1(\mod a^d - 1)$
Ainsi $a^r \equiv 1(\mod a^d - 1) \Rightarrow (a^d - 1)|(a^r - 1)$ absurde, car $r < d$ donc $r = 0$.

PROPOSITION 3.0.2 *(Sous-corps de $\mathbb{F}_{p^n}$)*

Un corps $\mathbb{F}_{p^n}$ possède un sous-corps de cardinal p^d si et seulement si $d|n$. Le cas échéant un tel sous-corps est unique, formé de l'ensemble des racines de $X^{p^d} - X$. Ce sous corps est noté $\mathbb{F}_{p^d}$.

Preuve

Si $\mathbb{F}_{p^d}$ est un sous-corps de $\mathbb{F}_{p^n}$, alors en particulier $F^*_{p^d}$ est un sous-groupe de $\mathbb{F}^*_{p^n} \implies p^d - 1 \mid p^n - 1$ alors $d \mid n$.

Réciproquement $d \mid n$, alors, avec les notations de la démonstration du lemme, on a :

$$\begin{aligned}
X^{p^n} - X &= X(X^{p^n - 1} - 1) \\
&= X(X^{p^{bd} - 1} - 1) \\
&= X(X^{(p^{(d)})^b - 1} - 1) \\
&= X(X^{(p^d - 1)N} - 1) \\
&= X[(X^{(p^d - 1)})^N - 1] \\
&= X[(X^{p^d - 1} - 1)((X^{(p^d - 1)})^{N-1} + \cdots + 1)] \\
&= (X^{p^d} - X)Q \text{ avec } Q = X^{(p^d - 1)^{N-1}} + \cdots + 1
\end{aligned}$$

Ce qui montre que $\mathbb{F}_{p^n}$ contient un corps de décomposition de $X^{p^d} - X$, (i.e une unique réalisation de $\mathbb{F}_{p^d}$. d'où $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$.

Exemple

Les sous corps strict de $\mathbb{F}_{16}$ sont $\mathbb{F}_2$ et $\mathbb{F}_4$. Notamment $\mathbb{F}_{16}$ n'a pas de sous corps à 8 éléments
Les sous corps strict de $\mathbb{F}_{65536} = \mathbb{F}_{2^{16}}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_{16}$ et $\mathbb{F}_{256}$.

LEMME 3.0.4

Soit L un corps fini contenant $\mathbb{F}_q$.

1) Pour tout $x \in L$, x appartient a $\mathbb{F}_q$ si et seulement si on a $x^q = x$

2) Pour tout $P(X) \in L[X]$, P(X) appartient a $\mathbb{F}_q[X]$ si et seulement si on a $P(X^q) = P(X)^q$.

REMARQUE 3.0.2

Concernant le 1) on peut appliquer la théorie de Galois à l'extension galoisienne L / $\mathbb{F}_q$, puisque $Gal(L\ /\ \mathbb{F}_q) = \{\sigma^j,\ 0 \leq j \leq deg(L) - 1\}$

Preuve

1) Soit x un élément de L. si x est dans $\mathbb{F}_q^*$, vu que $\mathbb{F}_q^*$ est un groupe d'ordre $q-1$, on a $x^{q-1} = 1$, d'ou $x^q = x$. Par ailleurs, le polynôme de $X^q - X \in L[X]$ possède au plus q racines dans $\mathbb{F}_q$ qui est l'ensemble de ses racines d'où l'assertion 1.

2) Soit $P(X) = \sum a_k X^k$ est un polynôme de L[X] on a

$$P(X)^q = (\sum a_k X^k)^q = \sum a_k^q X^{kq}$$

Cette dernière égalité se démontre comme de lemme(3.0.2) en procédant par récurrence sur le nombre de monôme de P. D'après la première assertion, P appartient à $\mathbb{F}_q$ si et seulement si $a_k^q = a_k$ pour tout k. Réciproquement si $P(X^q) = P(X)^q$, c'est à dire : $P(X)^q = (\sum a_k X^k)^q = \sum a_k^q X^{kq} = \sum a_k X^{kq}$ par identification on a $a_k^q = a_k$ pour tout k, donc $a_k \in \mathbb{F}_q$ alors $P(X) \in \mathbb{F}_q[X]$ d'où le résultat.

Notons que 2) du lemme est appelé **Lemme de Frobenius** [6]

THEOREME 3.0.3 *(Théorème de Werdderburn)*
Tout corps fini est commutatif.

Pour pouvoir démontrer le théorème de Werdderburn, nous allons énoncer le lemme suivant et la démonstration de ce lemme sera faite au chapitre 4.

LEMME 3.0.5

Soit $n > 1$.

Pour tout diviseur d de n distinct de n, le polynôme $\Phi_n(X)$ divise le polynôme $\dfrac{X^n - 1}{X^d - 1}$ dans $\mathbb{Z}[X]$.

Preuve

Soit F un corps fini, supposons que F soit non commutatif.
Le centre $Z = \{x \in F : \forall y \in F,\ xy = yx\}$ de F est un sous corps commutatif de F. Notons $card(Z) = q$. Soit p la caractéristique de Z. Alors Z est un $\mathbb{F}_p$-espace vectoriel de dimension finie $d = [F : \mathbb{F}_p]$, et $card(Z) = q = p^d$.

F est également un Z-espace vectoriel de dimension finie $n = [F : Z]$ alors $card(F) = q^n$.

Pour $x \in \mathbb{F}_p^*$, considérons $C(x) = \{y \in F : xy = yx\}$ alors $C(x)$ est un sous-corps de F contenant Z.
Donc $C(x)$ est un Z-espace vectoriel de dimension finie.
Notons $\delta(x) = [C(x) : Z]$ alors $Card(C(x)) = q^{\delta(x)}$.
On applique l'équation des classes au groupe multiplicatif F^* de cardinal $q^n - 1$ dont le centre n'est autre que Z^* de cardinal $q - 1$.

En remarquant que pour $x \in F^*$, $S_x = \{y \in F^* : xy = yx\}$ est le groupe multiplicatif $C(x)^*$ du corps $C(x)$. Alors $card(S_x) = q^{\delta(x)} - 1$. Par conséquent $q^{\delta(x)} - 1$ divise $q^n - 1$. Donc $\delta(x)$ divise n.

Notons que $\delta(x) = n$ équivaut à $x \in Z$.

On obtient donc :

$$q^n - 1 = q - 1 + \sum_{x \in \mathcal{R}} \frac{q^n - 1}{q^{\delta(x)} - 1} \quad (\star)$$

où x parcourt un ensemble $\mathcal{R}$ formé d'un représentant de chacune des classes non réduites à un singleton.

On a :

$$\begin{aligned} \mathcal{R} = \emptyset &\Leftrightarrow F = Z \\ &\Leftrightarrow [F : Z] = 1 \\ &\Leftrightarrow n = 1 \end{aligned}$$

Mais alors F serait commutatif et le résultat serait démontré.

Supposons le contraire c'est à dire que $n > 1$.

Comme $\Phi_n(q)$ divise $q^n - 1$ et que d'après le lemme précédant, $\Phi_n(q)$ divise chacun des termes de la somme de l'égalité $(\star)$, il len résulte que $\Phi_n(q)$ divise $q - 1$. D'où $|\Phi_n(q)| \leq q-1$. Mais $\Phi_n(q) = \prod_{\xi \in \mathcal{P}_n(\mathbb{C})} (q - \xi)$ où $\mathcal{P}_n(\mathbb{C})$ est l'ensemble des racines primitives n-ièmes de l'unité donc une partie du cercle unité $\mathbb{U}$ et Φ_n est le n-ième polynôme cyclotomique.

Pour chaque $\xi \in \mathcal{P}_n(\mathbb{C})$, $|q - \xi| \geq q - |\xi| = q - 1$, et l'égalité a lieu si et seulement si $\xi = 1$. Or, $n > 1$ donc un au moins des ξ de $\mathcal{P}_n(\mathbb{C})$ est différent de 1. Donc un au moins des facteurs $|q - \xi|$ est supérieur strictement à $q - 1$

$$|\Phi_n(q)| = \prod_{\xi \in \mathcal{P}_n(\mathbb{C})} |q - \xi| > \prod_{\xi \in \mathcal{P}_n(\mathbb{C})} |q - 1| = (q-1)^{\varphi(n)} > q - 1$$

En contradiction avec le fait que $|\Phi_n(q)| \leq q - 1$. Ainsi $n = 1$ et $F = Z$ donc F est commutatif.

DEFINITION 3.0.3 ***(élément primitif)***
On appelle racine primitive de $\mathbb{F}_q$ tout générateur du groupe multiplicatif $\mathbb{F}_q^*$.

THEOREME 3.0.4 ***(Théorème de l'élément primitif pour les corps finis)***
Toute extension finie d'un corps fini $\mathbb{F}_q$ est une extension simple, c'est à dire de la forme $\mathbb{F}_q(\alpha)$.

Preuve

Si $\mathbb{F}_q \subset \mathbb{F}_r$ et si α est une racine primitive de $\mathbb{F}_r$, alors $\mathbb{F}_r^* = \{1, \alpha, \alpha^2, ..., \alpha^{r-2}\}$ donc $\mathbb{F}_r = \mathbb{F}_q(\alpha)$.

3.1 Polynômes irréductible sur un corps fini

3.1.1 Clôture algébrique d'un corps fini

Commençons par observer que pour tout corps fini k, le polynôme $P(X) = 1 + \prod_{\alpha \in k}(X - \alpha)$ est sans racine dans k. Ainsi un corps fini ne saurait être algébriquement clos, car $P(\alpha) = 1$.

PROPOSITION 3.1.1

Le corps suivant : $\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$ est une clôture algébrique de tout corps fini de caractéristique p.

Preuve

Posons $\Omega = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{n!}}$. Ω est une union croissante de corps qui est donc naturellement munie d'une structure de corps et qui admet comme sous-corps n'importe quel corps fini de caractéristique p car $\mathbb{F}_{p^k} \subset \mathbb{F}_{p^{k!}} \subset \Omega = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{n!}}$, puisque $k \mid k!$

Soit $P(X) \in \Omega[X]$ irréductible, il existe $n \in \mathbb{N}$ tel que $P \in \mathbb{F}_{p^{n!}}[X]$. $P(X)$ admet donc une racine dans (corps de rupture) $\mathbb{F}_{p^{n!degp}} \subset \mathbb{F}_{p^{(ndegp)!}} \subset \Omega$. Ainsi Ω est algébriquement clos. Par définition de Ω, ses éléments sont tous algébriques sur $\mathbb{F}_p$ et Ω est donc une extension algébrique de n'importe quel corps fini de caractéristique p.

3.1.2 Polynômes irréductibles

Fixons un entier $q = p^r$, avec p premier et $r \in \mathbb{N}$. On note $I_u(n,q)$ l'ensemble des polynômes irréductibles et unitaires de degré n sur $\mathbb{F}_q$ et $m(n,q)$ le cardinal de cet ensemble.
commençons par un lemme qui caractérise les facteurs irréductibles du polynôme $X^{q^n} - X$.

LEMME 3.1.1
Soit $P(X) \in I_u(d,q)$, alors : $P(X)|(X^{q^n} - X)$ si et seulement $d|n$.

Preuve

Soit $P(X) \in I_u(d,q)$ un diviseur de $X^{q^n} - X$.
$\mathbb{F}_{q^n}$ est un corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$, par suite $P(X)$ y est scindé. Soit α une racine de $P(X)$ dans $\mathbb{F}_{q^n}$, on a alors $d = degP = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ qui divise $[\mathbb{F}_{q^n} : F_q] = n$. D'après le théorème de la base télescopique.

. Réciproquement, considérons α une racine de $P(X)$ dans une clôture algébrique de F_q, alors $\alpha \in \mathbb{F}_q(\alpha) = \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$, puisque $d|n$.
Ainsi α est aussi une racine de $X^{q^n} - X$ et $P(X) = \pi_{\alpha,\mathbb{F}_q} | X^{q^n} - X$, où $\pi_{\alpha,\mathbb{F}_q}$ est le polynôme minimal de α sur $\mathbb{F}_q$.

COROLLAIRE 3.1.1 *Sur un corps fini, les notions de corps de rupture et corps de décomposition coïncident.*

Preuve

Soit $P \in I_u(n,q)$, son corps de rupture est $\mathbb{F}_{q^n}$, qui est, d'après (le théorème sur l'existence et l'unicité) le corps de décomposition de $X^{q^n} - X$ d'où $P(X)|(X^{q^n} - X)$ et $P(X)$ est donc scindé dans $\mathbb{F}_{q^n}$.

PROPOSITION 3.1.2 *[6]*

- *Pour $n \in \mathbb{N}^*$, on a l'égalité suivante dans $\mathbb{F}_q[X]$:*

$$X^{q^n} - X = \prod_{d|n} \Big(\prod_{P(X)\in I_u(d,q)} P(X) \Big)$$

.

- $m(n,q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$

Preuve

. Soit d un diviseur de n, $P(X) \in I_u(d,q)$ et α une racine de $P(X)$ dans $\overline{\mathbb{F}_q}$, alors $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = d$ et donc $\mathbb{F}_q[\alpha]$ est isomorphe à $\mathbb{F}_{q^d}$. En particulier, α est racine de $X^{q^d} - X$ car $\mathbb{F}_{q^d}$ est le corps décomposition de ce polynôme. Or $X^{q^d} - X \mid (X^{q^n} - X)$ car $d \mid n$, donc α est aussi racine de $X^{q^n} - X$. En définitive toutes les racines de $P(X)$ sont aussi racine de $X^{q^n} - X$ et donc $P(X) \mid (X^{q^n} - X)$

Mais considérons des polynômes irréductibles $P(X) \neq Q(X) \in I_u(d,q)$ où $d \mid n$, alors ils n'ont aucune racine en commun, sinon ils représenteraient le polynôme irréductible d'un même élément : Par suite $(P(X), Q(X)) = 1 \Rightarrow P(X)Q(X) \mid (X^{q^n} - X)$., et donc :

$$\prod_{d|n} \Big(\prod_{P(X) \in I_u(d,q)} P(X) \Big) \mid (X^{q^n} - X)$$

.

. Inversement montrons que si $P(X)$ est diviseur irréductible de degré d de $X^{q^n} - X$, alors $d \mid n$.

Soit $P(X)$ un tel diviseur irréductible unitaire de $X^{q^n} - X$, soit ξ une de ses racines sur $\mathbb{F}_q^n$ ($P(X)$ y est scindé). Alors on a la tour d'extensions de corps $\mathbb{F}_q \subset \mathbb{F}_q(\xi) = \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n} \Rightarrow$ $d \mid n$. De plus, comme $X^{q^n} - X$ est à racines simples, chaque facteur irréductible n'apparait qu'une fois (nécessairement ils sont premiers entre eux). On en déduit que :

$$\prod_{d|n} \Big(\prod_{P(X) \in I_u(d,q)} P(X) \Big) = X^{q^n} - X$$

. En regardant les degrés dans l'égalité précédente on voit que $q^n = \sum_{d|n} d \times m(d,q)$.

Utilisons alors la formule de *Möbius* (cf. chapitre 2) on obtient : $m(n,q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$.

LEMME 3.1.2 *Soit k un corps et $P(X) \in k[X]$ de degré n. $P(X)$ est irréductible sur k si et seulement si $P(X)$ n'a pas de racines dans les extensions de k de degré inférieur à $\frac{n}{2}$.*

Preuve

Si $P(X)$ est irréductible sur k, le degré de $P(X)$ est le degré de la plus petite extension de k qui contienne une racine de $P(X)$, c'est un corps de rupture minimal de $P(X)$, or ce corps de rupture est une extension de k de degré n et c'est la plus petite qui contient une racine de P

Réciproquement, supposons que $P(X)$ soit tel que $P(X)$ n'ai aucune racine dans une extension de k de degré inférieur à $\frac{n}{2}$.Alors $P(X)$ n'est pas réductible car sinon un des ses facteurs irréductibles aurait pour corps de rupture un corps de degré $n/2 < d < n$ „ mais alors il existerait un facteur irréductible de $P(X)$ qui serait de degré $\leq n/2$, d'où une extension de degré $\leq n/2$ dans laquelle ce facteur (donc $P(X)$) y aurait une racine, ce qui est contradictoire à l'hypothèse. Donc $P(X)$ est irréductible.

DEFINITION 3.1.1

(La complexité)

La complexité estime le temps de calcul (pour un nombre d'opérations élémentaires dépendant d'un nombre n ou de plusieurs) nécessaire pour effectuer une opération ($+, \div, \times ...$) à partir des bits ou chiffres en base 2 le composant. Il suffit de calculer le "petit o" de la fonction de calcul. Il y a 2 types de complexité : A savoir Exponentielle et polynomiale. Celle de type exponentielle ne peut pas donner le résultat en un temps raisonnable.

COROLLAIRE 3.1.2 ***(Test de Rabin.)***

Soit $P(X) \in \mathbb{F}_q[X]$ de degré $n \in \mathbb{N}^*$, alors :

$P(X)$ est irréductible sur $\mathbb{F}_q$ si et seulement si $P(X)$ divise $X^{q^n} - X$ et si, pour tout diviseur strict d de n, $P(X)$ et $X^{q^d} - X$ sont premier entre eux.

REMARQUE 3.1.1

Conséquences : On peut également remplacer la seconde assertion par : "$\forall r$ premier et r / n alors $(P(X)$, $X^{q^{n/r}} - X) = 1$".

Les polynômes irréductibles de $\mathbb{F}_q[X]$ de degré n sont donc exactement les facteurs irréductibles de $X^{q^n} - X$ qui sont premiers à $X^{q^d} - X$, pour tout diviseur strict d de n.

Preuve

Supposons que $P(X)$ soit irréductible. Comme il est de degré n et n/n, alors on a le 1er point : $P(X) \mid (X^{q^n} - X)$.

Par ailleurs, si l'on suppose que $(P(X)\ , X^{q^d} - X) = G(X) \neq 1$ alors nécessairement $G(X) = P(X)$ car $P(X)$ est irréductible et $\mathbb{F}_q[X]$ est factoriel, donc $P(X) | (X^{q^d} - X)$ et par suite toutes ses racines sont dans une extension de degré $d \leq n/2$, ce qui d'après le Lemme précédent signifierait que P(X) est réductible, ce qui est contradictoire à l'hypothèse.

Réciproquement : Soit $P(X)$ un polynôme de degré n tel que : $P(X) \mid (X^{q^n} - X)$ et $(P(X)\ , X^{q^d} - X\ ) = 1\ , \forall\ d \neq n$ et $d\ /\ n$.

On montre que $P(X)$ est irréductible.

Il est clair que $P(X)$ a toutes ses racines dans $\mathbb{F}_{q^n}$ de même que tous ses facteurs irréductibles $P_i(X)$ qui du fait que $X^{q^n} - X$ soit scindé réalisent $(\ P_i(X),\ P_j(X)) = 1$ si $i \neq j$ et $P(X) = \prod_{i=1}^{s} P_i(X)$. Notons aussi que si d_i est le degré de $P_i(X)$ alors $\mathbb{F}_{q^{d_i}} \subset \mathbb{F}_{q^n}$ ce qui montre que d_i/n .

Par ailleurs, on a supposé également que $(\prod_{i=1}^{s} P_i(X),\ X^{q^d} - X) = 1\ ,\ \forall d \neq n$ et $d\ /\ n$, on en déduit que $\forall i = 1, ..., s\ (P_i(X),\ X^{q^d} - X) = 1\ ,\ \forall\ d \neq n$ et $d\ /\ n$, on en déduit que $\mathbb{F}_{q^{d_i}} \nsubseteq \mathbb{F}_{q^d} \Rightarrow d_i \nmid d$. Or d_i est un diviseur strict de n et $\exists d\ / d = d_i$. Donc $P(X)$ est irréductible.

REMARQUE 3.1.2 *[6]*

La fonction de Möbius μ permet de donner une expression exacte de nombre de polynôme de degré n irréductible sur $\mathbb{F}_q$, i.e une expression exacte p pour $m(n,q)$ et on a :

$m(n,q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$.

Exemple

Donnons le nombre de polynômes irréductibles de degré 2 sur $\mathbb{F}_2$.

D'abord on a 2^2 polynômes de degré 2 sur $\mathbb{F}_2[X]$:X^2, $X^2 + 1$, $X^2 + X$, $X^2 + X + 1$. $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$. En appliquant la remarque on a :

$$m(2,2) = \frac{1}{2} \sum_{d|2} \mu(\frac{2}{d}) 2^d = \frac{1}{2}(\mu(2)2 + \mu(1)2^2) = \frac{1}{2}(-2 + 2^2) = 1$$

et on vérifie rapidement que c'est l'unique polynôme $X^2 + X + 1$.

Déterminons le nombre de polynôme irréductible de degré 3 sur F_2.

on a 2^3 polynômes de degré 3 sur $\mathbb{F}_2[X]$: X^3, $X^3 + 1$, $X^3 + X$, $X^3 + X + 1$, $X^3 + X^2$, $X^3 + X^2 + 1$, $X^3 + X^2 + X$, $X^3 + X^2 + X + 1$.

En appliquant la formule

$$m(3,2) = \frac{1}{3} \sum_{d|3} \mu(\frac{3}{d}) 2^d = \frac{1}{3}(\mu(3)2 + \mu(1)2^3) = \frac{1}{3}(-2 + 2^3) = \frac{6}{3} = 2$$

$\boxed{m(3,2) = 2}$

on vérifie rapidement qu'il s'agit de $X^3 + X^2 + 1$ et $X^3 + X + 1$

LEMME 3.1.3

Soit $F = F_1 \cdots F_r \in \mathbb{K}[X]$ et $G = G_1 \cdots G_k \in \mathbb{K}[X]$ sans facteurs multiples où les F_i sont deux à deux premiers entre eux, de même pour les G_i. Alors

$$pgcd(F, G) = \prod_{i=1}^{k} pgcd(F, G_j) = \prod_{j=1}^{r} pgcd(F_i, G)$$

.

Chapitre 4

Décomposition des polynômes et leur factorisation sur les corps finis

4.1 Algorithme de Berlekamp

4.1.1 Approche Déterministe

Soit $p \in \mathcal{P}$ et $q = p^s$. On considère $P(X) \in \mathbb{F}_q[X]$ sans facteurs carrés que l'on écrit $P(X) = \prod_{i=1}^{r} P_i(X)$, les $P_i(X)$ étant irréductibles sur $\mathbb{F}_q[X]$ et premiers entre eux deux à deux. L'intérêt de l'algorithme de Berlekamp est de calculer le nombre r de facteurs irréductibles de $P(X)$, et lorsque $r \geqslant 2$ comme étant la dimension d'une $\mathbb{F}_q$-algèbre de dimension finie, et de donner toujours en utilisant cette algèbre, explicitement les $P_i(X)$, i.e la factorisation de $P(X)$.

On pose $A = \mathbb{F}_q[X]/(P(X))$, alors A est une $\mathbb{F}_q$-algèbre de dimension finie où $dim_{\mathbb{F}_q}(A) = deg(P) = n$ car $\bar{Q} \in A$ est alors représenté par un unique polynôme $R(X)$ tel que $R(X) = 0$ ou $deg(R(X)) \leqslant n-1$, obtenu par division euclidienne de $Q(X)$ par $P(X)$ dans l'anneau euclidien $\mathbb{F}_q[X]$.

L'idée de Berlekamp fut de se donner une autre algèbre représentée par les éléments de l'algèbre précédente qui sont <u>invariants</u> par l'élévation à la puissance q, c'est-à -dire invariants sous l'action de la s-ème itérée du morphisme de Frobenius associé à cette algèbre A.
On introduit alors

$$\begin{gathered}\mathcal{F} : A \longrightarrow A \\ \bar{Q}(X) = Q(X) \mod (P(X)) \longmapsto \bar{Q}(X)^q = Q(X)^q \mod (P(X))\end{gathered}$$

le morphisme d'élévation à la puissance q.

DEFINITION 4.1.1 *On définit l'algèbre de Berlekamp par :*

$$A^{\mathcal{F}} = \left\{\bar{Q}(X) \in A \ / \ \bar{Q}(X)^q = \bar{Q}(X)\right\} = Ker(\mathcal{F} - Id_A)$$

.

PROPOSITION 4.1.1
Pour tout $\bar{Q}(X) \in A^{\mathcal{F}}$; il existe un unique r-uplet $(c_1, \cdots, c_r) \in \mathbb{F}_q^r$ tels que $Q(X) \equiv c_i \mod P_i(X)$ et $(c_1, \cdots, c_r) = (c, \cdots, c)$ est un r-uplet constant si et seulement s'il existe $c \in \mathbb{F}_q$ tel que $Q(X) \equiv c \mod (P(X))$. Alors $r = dim_{\mathbb{F}_q}(A)^{\mathcal{F}}$ est exactement le nombre de facteurs irréductibles de $P(X)$; et $A^{\mathcal{F}} \cong \mathbb{F}_q^r$ en tant que $\mathbb{F}_q$algèbre.

Preuve

Etape 1 : le théorème chinois assure que $\mathbb{F}_q[X]/(P) \simeq \mathbb{F}_q[X]/(P_1(X)) \times \cdots \times \mathbb{F}_q[X]/(P_r(X)) \cong \mathbb{F}_q[\alpha_{11}] \times \cdots \times \mathbb{F}_q[\alpha_{r1}]$, où α_{k1} est une racine quelconque de $P_1(X)$, et ce, via l'application :

$$\phi : \mathbb{F}_q[X]/(P(X)) \longrightarrow \mathbb{F}_q[X]/(P_1(X)) \times \cdots \times \mathbb{F}_q[X]/(P_r(X))$$
$$\bar{Q}(X) = Q(X) \mod P(X) \longmapsto (Q(X) \mod P_1(X), \cdots, Q \mod P_r(X)) = (Q(\alpha_{11}), \cdots, Q(\alpha_{r1})$$

où chaque $\mathbb{F}_q[X]/(P_i(X)) = \mathbb{K}_i = \mathbb{F}_q[\alpha_{i1}]$ est un corps fini de cardinal $q^{degP_i(X)}$, puisque $P_i(X)$ est irréductible.

En particulier $\mathbb{K}_i$ est une extension de $\mathbb{F}_q$ de dimension $n_i = deg(P_i(X))$ et on note :

$$\mathcal{F}_i : \mathbb{K}_i \longrightarrow \mathbb{K}_i$$
$$Q \mod P_i(X) \longmapsto Q(X)^q \mod P_i(X) \text{ (soit } Q(\alpha_{i1}) \longmapsto Q(\alpha_{i1})^q$$

Par le théorème chinois, ϕ est bijective et on a donc $\bar{Q}(X) \in A^{\mathcal{F}} \Leftrightarrow \bar{Q}(X)^q = \bar{Q}(X)$ dans $A = \mathbb{F}_q[X]/(P(X)) \Leftrightarrow \phi(\bar{Q}(X)^q) = \phi(\bar{Q}(X))$ dans $\mathbb{F}_q[X]/(P_1(X)) \times \cdots \times \mathbb{F}_q[X]/(P_r(X))$ et donc

$$\bar{Q} \in A^{\mathcal{F}} \Longleftrightarrow \bar{Q}(X)^q = \bar{Q}(X) \text{ dans } \mathbb{F}_q[X]/(P_i(X)), \forall i \in \overline{1:r} \Leftrightarrow Q \mod P_i \in \mathbb{K}_i^{\mathcal{F}_i}, \forall i \in \overline{1:r}.$$

objectif : Montrons que $\mathbb{K}_i^{\mathcal{F}_i} = \mathbb{F}_q$.

$\mathbb{K}_i^{\mathcal{F}_i} = \{\bar{Q}(X) \in \mathbb{F}_q[X]/(P_i(X) \ / \ \bar{Q}(X)^q = \bar{Q}(X)\} = Ker(\mathcal{F}_i - Id_{\mathbb{K}_i})$ soit aussi $= \{Q(\alpha_{i1}) \in \mathbb{F}_q[\alpha_{i1}] \ / \ Q(\alpha_{i1})^q = Q(\alpha_i$ (via le Lemme 3.0.4).

Montrons le avec l définition de base : $\mathbb{K}_i^{\mathcal{F}_i}$ est une $\mathbb{F}_q$ extension donc $\mathbb{F}_q \subset \mathbb{K}_i^{\mathcal{F}_i}$ Réciproquement pour tout $\bar{Q}(X) \in \mathbb{K}_i^{\mathcal{F}_i}$, on a $\bar{Q}(X)^q = \bar{Q}(X)$ d'après le lemme(3.0.4) $\mathbb{K}^{\mathcal{F}_i} \subset \mathbb{F}_q$.

On en déduit donc que $\bar{Q} \in A^{\mathcal{F}}$ si et seulement si pour tout $i \in \overline{1:r}$, $(Q(X) \mod P_i(X) = c_i \in \mathbb{F}_q$ i.e $Q(X) = c_i \mod P_i(X)$; On en conclut donc que :

$$\bar{Q}(X) \in A^{\mathcal{F}} \Longleftrightarrow \exists!(c_1, \cdots, c_r) \in \mathbb{F}_q^r / \ Q(X) \equiv c_i \mod P_i(X), \forall i \in \overline{1:r}$$

conclusion Etape 1 : ϕ induit un isomorphisme de $A^{\mathcal{F}}$ sur $\mathbb{F}_q^r$ et $dim_{\mathbb{F}_q}(A^{\mathcal{F}}) = dim_{\mathbb{F}_q}(\mathbb{F}_q^r) = r$ est le nombre de facteurs irréductibles de $P(X)$.

Etape 2 : Si $\bar{Q}(X) \in A^{\mathcal{F}}$, d'après ce qui précède il existe un unique r-uplet $(c_1, \cdots, c_r)$ tel que $Q(X) \equiv c_i \mod P_i(X)$.

Si maintenant $Q(X) \equiv c \mod (P(X))$., alors $P(X)|(Q(X) - c)$ et pour tout $i \in \overline{1:r}$, $P_i(X)|(Q(X) - c)$ d'où $Q(X) \mod P_i(X) = c_i$ et par unicité de $(c_1, \cdots, c_r)$, on a $c_i = c$ pour tout $i \in \overline{1:r}$.

réciproquement si $(c, \cdots, c) = (c_1, \cdots, c_r)$, alors $Q(X) \mod P_i(X) = c$, soit $P_i(X)|(Q(X) - c)$ pour tout $i \in \overline{1:r}$ et comme les $P_i(X)$ sont premiers entre eux donc $P(X)|(Q(X) - c)$ et $Q(X) \mod P(X) = c$.

REMARQUE 4.1.1 *On en déduit que $dim_{\mathbb{F}_q}(A^{\mathcal{F}}) = r$ et $P(X)$ est irréductible$\Longleftrightarrow dim_{\mathbb{F}_q}(A^{\mathcal{F}}) = 1$ (qui est égal aux nombres de facteurs irréductibles de $P(X)$).*

DEFINITION 4.1.2

La matrice de Berlekamp $M = (m_{i,j})_{1 \leq i,j \leq n}$ représente la matrice de l'endomorphisme $\mathcal{F} - Id_A$ dans la base canonique $(x^i)_{0 \leq i \leq n-1}$ de A où $x = \bar{X} = X \mod P(X)$.

THEOREME 4.1.1

$rg(M) \leq n-1$ et pour $r > 1$, il existe $\bar{G}(X)$ non constant dans $A^{\mathcal{F}}$ et une décomposition non triviale de $P(X)$ donnée par :

$$P(X) = \prod_{\alpha \in \mathbb{F}_q} pgcd(P(X), G(X) - \alpha). \ (*)$$

Preuve

Etape 1 : Comme $\bar{1} \in \mathbb{F}$ vérifie $\bar{1}^q = \bar{1}$, on a $(\mathcal{F} - id_A)(\bar{1}) = 0$ et la première colonne de la matrice est nulle, ce qui donne $rg(\mathcal{F} - Id_A) \leq n-1$. D'après le théorème du rang on obtient $dim_{\mathbb{F}_q}(Ker(\mathcal{F} - Id_A)) = dim_{\mathbb{F}_q}(A^{\mathcal{F}}) \geq 1$.

Etape 2 : On suppose $r > 1$, alors l'ensemble des $\bar{Q}(X)$ tel que $\bar{Q}(X) = c$ lorsque $c \in \mathbb{F}_q$ est la droite vectorielle de $A = \mathbb{F}_q[X]/(P(X))$ engendrée par $1_{\mathbb{F}_q}$ et est donc de dimension 1, or $dim_{\mathbb{F}_q}(A^{\mathcal{F}}) = r > 1$, il existe nécessairement dans $A^{\mathcal{F}}$ un élément $\bar{G}(X)$ non constant ; Montrons à présent la décomposition annoncée. On a $X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$ ce qui nous donne pour $G \in \mathbb{F}_q[X]$ non constant, on obtient par substitution :

$$G(X)^q - G(X) = \prod_{\alpha \in \mathbb{F}_q} (G(X) - \alpha)$$

. On remarque alors que les $G(X) - \alpha$, sont deux à deux premiers entre eux, sinon pour $\alpha_1 \neq \alpha_2 \in \mathbb{F}_q$, $g(X) - \alpha_1$ et $G(X) - \alpha_2$ aurait une racine commune c dans une certaine extension de $\mathbb{F}_q$, ce qui donnerait $G(c) - \alpha_1 = G(c) - \alpha_2 = 0$ alors $\alpha_1 = \alpha_2$, absurde. Ainsi, $P(X)$ et $G(X)^p - G(X)$ sont tous les deux sans facteurs multiples, ce qui donne bien d'après le lemme(3.1.3) :

$$pgcd(P(X), G(X)^q - G(X) = \prod_{\alpha \in \mathbb{F}_q} pgcd(P(X), G(X) - \alpha)$$

Comme $\bar{G}(X) \in A^{\mathcal{F}}$, $P(X) | G(X)^q - G(X)$ et donc à gauche : $pgcd(P(X), G(X)^q - G(X) = P(X)$. Il est important de noter que cette décomposition est non trivial. En effet sinon il existerait un $\alpha \in \mathbb{F}_q$ tel que $pgcd(P(X), G(X) - \alpha) = P(X)$ et on aurait $P(X) | (G(X) - \alpha)$, alors $\bar{G} = \alpha$ dans $A = \mathbb{F}_q[X]/(P(X))$ et $\bar{G}(X)$ serait constant, absurde.
Il s'agit désormais d'obtenir la factorisation de $P(X)$ en produits de polynômes irréductibles.

THEOREME 4.1.2 ***algorithme de Berlekamp***
Le processus suivant se termine en un nombre fini d'étapes et donne la décomposition en facteurs irréductibles de $P(X)$:

1. *On détermine la matrice de Berlekamp M dans la base canonique de A, puis on passe au 2.*
2. *le nombre de facteurs irréductibles de P est $r = n - rg(M) = dim(ker(M))$. Si $r = 1$, alors P est irréductible et on arrête l'algorithme, sinon on passe à l'étape 3 suivante.*
3. *On détermine un polynôme Q non congru modulo P à un polynôme constant de $\mathbb{F}_q[X]$ et tel que $\bar{Q}(X) \in ker(M) = A^{\mathcal{F}}$. Avec l'algorithme d'Euclide, on calcule alors les $pgcd(P(X), Q(X) - \alpha)$ pour $\alpha \in \mathbb{F}_q$ et on a alors :*

$$P(X) = \prod_{\alpha \in \mathbb{F}_q} pgcd(P(X), Q(X) - \alpha) \qquad (*)$$

.

On retourne ensuite au 1 avec chacun des facteurs non triviaux de $(*)$.

Preuve

D'après tout ce qui précède, il suffit de montrer que l'algorithme se termine et donc que le nombre de facteurs irréductibles diminue à chaque étape. Si $P(X)$ n'est pas irréductible, une décomposition du type (*) existe bien et cette décomposition n'est pas triviale. les facteurs non triviaux qui la composent ont donc strictement moins de facteurs irréductibles que P et comme ce sont des diviseurs de P, sont clairement sans facteurs carrés.

4.1.2 Principe de l'algorithme de Berlekamp

Soit $K = \mathbb{F}_q$ un corps fini, et soit $P(X) \in K[X]$ un polynôme. On souhaite factoriser P ; l'algorithme de Berlekamp prend P en entrée, et ressort soit P si celui-ci est irréductible, soit un diviseur non trivial de P. Les étapes sont les suivantes :

(1) si $P(X)' = 0$ alors il existe $Q \in K[X]$, tel que $P(X) = Q(X^p)$. Soit R le polynôme dont les coefficients sont les racines p-ième des coefficients de Q (bien déterminés car le Frobenius F est un isomorphisme de k), alors $P(X) = (R(X))^p$ et l'algorithme renvoie R et s'arrête.

(2) si $P(X)' \neq 0$ et $pgcd(P(X), P'(X) \neq 1$ alors c'est un facteur non trivial de $P(X)$ donc l'algorithme renvoie $pgcd(P(X), P('X)$ et s'arrête.

(3) si $P(X)' \neq 0$ et $pgcd(P(X), P'(X) = 1$, $P(X)$ a ses facteurs irréductibles distincts. Soit $A = K[X]/(P(X))$ qui est une K-algèbre de dimension n, et considérons l'endomorphisme de K-algèbre $\mathcal{F} - id_A$. Soit r la dimension de $N = ker(\mathcal{F} - id_A)$; on a $r \geq 1$ car $K \subset N$. Si $r = 1$ alors $P(X)$ est irréductible, l'algorithme le dit et s'arrête. Si $r \geq 2$ on prend un élément de $N \setminus K$, classe d'un polynôme $Q \in K[X]$. On décrit alors tous les $\alpha \in K$ et on calcule le pgcd de P et $Q - \alpha$.

Mise en pratique

Factoriser : $P(X) = X^9 + X^6 - X + 1$ sur $K = \mathbb{F}_3$.

La première chose à faire est de voir s'il a une racine dans K. C'est vite fait car K n'a que 3 éléments, et on trouve qu'il n'y a pas de racine. Appliquons maintenant l'algorithme :

(1) $P'(X) = -1$.

(2) $pgcd(P(X), P'(X)) = 1$ car $P' = -1$.

(3) L'algèbre qui nous intéresse est :

$$A = \mathbb{F}_3[X]/(X^9 + X^6 - X + 1).$$

c'est un $\mathbb{F}_3$-ev de dimension 9 dont une base est la classe de $\{1, X, X^2, \cdots, X^8\}$,mais pour simplifier on conserve cette notation. Pour calculer la matrice de l'endomorphisme $\mathcal{F} - id_A$ on aura besoin des puissances de X^{3i} jusqu'à X^{24}. Néanmoins je vais calculer aussi X^{10} et X^{11}, ce qui va faciliter le calcul :

$X^9 = -X^6 + X - 1$
$X^{10} = -X^7 + X^2 - X$
$X^{11} = -X^8 + X^3 - X^2$
$X^{12} = -(-X^6 + X - 1) + X^4 - X^3 = X^6 + X^4 - X^3 - X + 1$
$X^{15} = (-X^6 + X - 1) + X^7 - X^6 - X^4 + X^3 = X^7 + X^6 - X^4 + X^3 + X - 1$
$X^{18} = (-X^7 + X^2 - X) + (-X^6 + X - 1) - X^7 - X^6 - X^4 - X^3 = X^7 + X^4 - X^3 + X^2 - 1$
$X^{21} = (-X^7 + X^2 - X) + X^7 - X^6 + X^5 - X^3 = -X^6 + X^5 - X^3 + X^2 - X$
$X^{24} = -(-X^6 + X - 1) + X^8 - X^6 + X^5 - X^4 = X^8 + X^5 - X^4 - X + 1$

On peut alors écrire la matrice de $\mathcal{F} - id_A$:

$$\begin{pmatrix} 0 & 0 & 0 & -1 & 1 & -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 1 & -1 & 1 & 0 & -1 & -1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & -1 & -1 & 1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ X \\ X^2 \\ X^3 \\ X^4 \\ X^5 \\ X^6 \\ X^7 \\ X^8 \end{matrix}$$

Le noyau contient la droite engendrée par la première colonne ; il faut décider s'il est plus gros. Utilisons le pivot de Gauss ; c'est long mais on trouve le vecteur $(0, 1, -1, -1, 1, 1, -1, 0, 1)$ (par exemple). Un représentant polynôme est

$$Q(X) = X^8 - X^6 + X^5 + X^4 - X^3 - X^2 + X$$

On calcule ensuite $pgcd(P(X), Q(X) - \alpha)$. Gardons α général au début, on fera $\alpha = 0$, 1 ou 2 en temps utile. On utilise l'algorithme d'Euclide : la première division est

$$X^9 + X^6 - X + 1 = X(X^8 - X^6 + X^5 + X^4 - X^3 - X^2 + X - \alpha) + (X^7 - X^5 + X^4 + X^3 - X^2 + (\alpha - 1)X + 1)$$

La seconde est

$$X^8 - X^6 + X^5 + X^4 - X^3 - X^2 + X - \alpha = (X^7 - X^5 + X^4 + X^3 - x^2 + (\alpha - 1)X + 1)X - \alpha(X^2 + 1)$$

C'est gagné car si $\alpha = 0$, on a un reste nul, donc $X^7 - X^5 + X^4 + X^3 - X^2 - X + 1$ divise $P(X)$:

$$P(X) = (X^7 - X^5 + X^4 + X^3 - X^2 - X + 1)(X^2 + 1)$$

Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{F}_3$. Il faut ensuite recommencer avec le facteur $P_1 = X^7 - X^5 + X^4 + X^3 - X^2 - X + 1$. Intéressons nous maintenant à l'algèbre noté encore A. $A = \dfrac{\mathbb{F}_3[X]}{(X^7 - X^5 + X^4 + X^3 - X^2 - X + 1)}$ c'est un $\mathbb{F}_3$-ev de dimension 6 dont une base est $\{1, X, X^2, X^3, X^4, X^5, X^6\}$. Calculons la matrice de l'endomorphisme $\mathcal{F} - id_A$: on aura besoin des puissances $X^{3i} \mod P(X)$ pour $0 \leq i \leq 6$

$$\begin{matrix} X^7 = X^5 - X^4 - X^3 + X^2 + X - 1 \\ X^9 = -X^6 + X - 1 \\ X^{12} = X^6 + X^4 - X^3 - X + 1 \\ X^{15} = -X^6 + X^5 + X^4 + X^2 - X + 1 \\ X^{18} = X^5 + X^3 - X^2) + X + 1 \end{matrix} \qquad \begin{pmatrix} & & & Matrice & de & F - Id & \\ 0 & 0 & 0 & -1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & -1 & 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & -1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} \begin{matrix} 1 \\ X \\ X^2 \\ X^3 \\ X^4 \\ X^5 \\ X^6 \end{matrix}$$

Ici on voit rapidement que le système formé par les six colonnes de droite est de rang maximal, donc la dimension du noyau est 1 et $P(X)$ est irréductible. en conclusion la décomposition en facteurs irréductibles sur $\mathbb{F}_3[X]$ de $X^9 + X^6 - X + 1$ est $(X^7 - X^5 + X^4 + X^3 - X^2 - X + 1)(X^2 + 1)$.

L'exemple précédent nécessite l'aide de certains logiciels de calculs formels tels que PARI GP, MAPLE, MATHEMATICA, SAGE.

Nous allons maintenant voir un autre exemple, où tous les calculs peuvent être effectuer à la main
Exemple : Factoriser le polynôme $P(X) = X^4 + X^2 + X + 1$ sur le corps $\mathbb{F}_2$

$P'(X) = 4X^3 + 2X + 1 = 1$; donc le $pgcd(P(X), P'(X)) = 1$ alors $P(X)$ est sans facteur multiple
Intéressons-nous maintenant à l'algèbre
$A = \dfrac{\mathbb{F}_2[X]}{(X^4 + X^2 + X + 1)}$ c'est un $\mathbb{F}_2$-ev de dimension 4 dont une base est $\{1, X, X^2, X^3\}$. Calculons la matrice de l'endomorphisme $\mathcal{F} - Id_A$ on aura besoin des puissances $X^{2i} \mod P(X)$ pour $0 \leq i \leq 3$

$$\begin{aligned} X^0 &\equiv 1 \mod P(X) \\ X^2 &\equiv X^2 \mod P(X) \\ X^4 &\equiv 1 + X + X^2 \mod P(X) \\ X^6 &\equiv 1 + X + X^3 \mod P(X) \end{aligned}$$

$$\begin{aligned} (\mathcal{F} - Id_A)(1) &= 1^2 - 1 = 0 \\ (\mathcal{F} - Id_A)(X) &= X^2 - X = X^2 - X \\ (\mathcal{F} - Id_A)(X^2) &= 1 + X + X^2 - X^2 = 1 + X \\ (\mathcal{F} - Id_A)(X^3) &= 1 + X + X^3 - X^3 = 1 + X \end{aligned}$$

La matrice de l'endomorphisme est :

$$M = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ & & & \end{pmatrix}$$

Le rang de la matrice est exactement $r = 2$ par conséquent $P(X)$ admet $k = 4 - 2 = 2$ facteurs unitaires irréductibles distincts.
Le noyau de cette matrice est engendré par deux vecteurs qui sont $(1, 0, 0, 0)$ et $(0, 0, 1, 1)$, les représentants polynômes sont $H_1(X) = 1$ et $H_2(X) = X^2 + X^3$
Maintenant en utilisant le théorème (4.1.1) calculons :

$$\begin{aligned} pgcd(P(X), H_2(X) - 0) &= X + 1 \\ pgcd(P(X), H_2(X) - 1) &= X^3 + X^2 + 1 \end{aligned}$$

Remarquons que le polynôme $X^3 + X^2 + 1$ est irréductible sur $\mathbb{F}_2$ car aucun élément de $\mathbb{F}_2$ ne l'annule alors :
$P(X) = (X + 1)(X^3 + X^2 + 1)$ est la décomposition enfacteurs irréductible sur $\mathbb{F}_2[X]$ de $P(X)$.

L'approche précédente requiert de calculer $pgcd(P(X), G(X) - w)$ pour $\overline{G}$ non constant dans $A^{\mathcal{F}}$ et w parcourant $\mathbb{F}_p$. La complexité est au moins linéaire en p et l'algorithme s'avère vite impraticable lorsque p est grand. Il existe une autre approche probabiliste plus performante pour p grand.

4.1.3 Approche Probabiliste (décomposition sur $\mathbb{F}_p[X]$)

Plutôt que de chercher les facteurs de $P(X)$ parmi les facteurs $G(X)-\alpha$ de $G^p(X)-G(X)$, nous allons utiliser la factorisation :

$$G^p(X)-G(X)=G(X)(G^{\frac{p-1}{2}}(X)-1)(G^{\frac{p-1}{2}}(X)+1)$$

valable pour tout nombre premier $p\neq 2$. On a alors $\overline{G}(X)\in A^{\mathcal{F}}\Leftrightarrow P(X)$ divise $G^p(X)-G(X)$, par conséquent :

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

Si $G(X)\neq 0$ et $G_1(X)=pgcd(P(X),G(X))\neq 1$, alors on a trouvé un facteur $G_1(X)$ non trivial de $P(X)$ et on rappelle l'algorithme récursivement sur $G_1(X)$ d'une part et sur $P(X)/G_1(X)$ d'autre part.

Si $G_1(X)$ =1, alors $G_2(X)=pgcd(P(X),G^{\frac{p-1}{2}}(X)-1)=P(X)$ si et seulement si :

$$G^{\frac{p-1}{2}}(X)-1\equiv 0 \mod (P_i(X)),\forall i=1\cdots s$$

et $G_2(X)$ =1 alors $G_3(X)=pgcd(P(X),G^{\frac{p-1}{2}}(X)+1)=P(X)$ si et seulement si

$$G^{\frac{p-1}{2}}(X)+1\equiv 0 \mod (P_i(X)),\forall i=1\cdots s$$

Le lemme suivant montre que ces deux situations de factorisations triviale $G_2(X)\in\{1,P\}$ n'arrivent qu'avec une faible probabilité

LEMME 4.1.1 *Soit $p\neq 2$ un nombre premier. Les deux sous -ensembles*
$S_+=\{z\in {\mathbb{F}_p}^*, z^{\frac{p-1}{2}}-1=0\}$ *et* $S_-=\{z\in {\mathbb{F}_p}^*, z^{\frac{p-1}{2}}+1=0\}$
sont de même cardinal $(p-1)/2$ et réalisent une partition de ${\mathbb{F}_p}^*$

Preuve

On a : $0=z^{p-1}-1=(z^{\frac{p-1}{2}}-1)(z^{\frac{p-1}{2}}+1)$, $\forall z\in {\mathbb{F}_p}^*$

la deuxième égalité utilisant l'hypothèse p impair, on a donc une partition de ${\mathbb{F}_p}^*=S_+\cup S_-$ et il s'ensuit que

$$Card(S_+)+Card(S_-)=Card({\mathbb{F}_p}^*)=p-1.$$

D autre part, les polynômes $X^{(p-1)/2}-1$ et $X^{(p-1)/2}+1$ de ${\mathbb{F}_p}^*[X]$ ont chacun au plus $(p-1)/2$ racines et ainsi

$$Card(S_+)\leq\frac{p-1}{2}\quad et\quad Card(S_-)\leq\frac{p-1}{2}$$

En combinant (4.4) et (4.5) on obtient que $Card(S_+)=\frac{p-1}{2}$ et $Card(S_-)=\frac{p-1}{2}$

Rappelons que $\overline{G}(X)\in A^{\mathcal{F}}$ si et seulement si $G(X) \mod P_i(X)\in\mathbb{F}_p$ pour tout $i=1\cdots s$. Ainsi, si $\overline{G}\in A^{\mathcal{F}}$ est combinaison linéaire des éléments d'une base de $A^{\mathcal{F}}$ à coefficients dans $\mathbb{F}_p$ aléatoires, alors $G \mod P_i(X)\in\mathbb{F}_p$ prend chaque valeur de $\mathbb{F}_p$ avec une probabilité 1/p, et cela pour tout $i=1\cdots s$. Il suit du lemme précédent, que si $G(X) \mod P_i(X)\neq 0$, alors les deux événements $G^{\frac{p-1}{2}}(X)-1\equiv 0 \mod P_i(X)$ et $G^{\frac{p-1}{2}}(X)+1\equiv 0 \mod P_i(X)$ ont une équiprobabilité de 1/2. Ainsi chaque événement (4.3) et (4.4) apparait avec une probabilité $1/2^s$. Donc G_2 est un facteur trivial avec une probabilité $1/2^{s-1}$, quantité inférieur ou égale à 1/2 des lors que $s\geq 2$. si G_2 est un facteur trivial, on recommence avec un autre choix de G .La probabilité de n'obtenir que des facteurs triviaux après k itérations vaut

$$\frac{1}{2^{k(s-1)}}\leq\frac{1}{2^k}$$

et la probabilité de trouver une factorisation non trivial de P(X) tend vers 1 lorsque k tend vers l'infini .
En pratique, 1 ou 2 itérations suffissent, et l'approche probabiliste aura une meilleure complexité en moyenne que l'approche déterministe.

4.2 Algorithme de Cantor-Zassenhauss

Nous avons vu la méthode de Berlekamp, essentiellement basée sur l'algèbre linéaire. On va maintenant voir une méthode connue et fréquemment utilisée, la méthode de Cantor-Zassenhauss.
Elle consiste dans un premier temps à regrouper les facteurs de même degré
(**distinct degree factorization**) puis à factoriser ces groupes selon une méthode probabiliste similaire à celle développer ci-dessus. Commençons par une remarque simple sur la recherche de racines.

4.2.1 Recherche de racines

L'algorithme précédant admet comme application immédiate la recherche des racines d'un polynôme $P(X) \in \mathbb{F}_p[X]$ sans facteurs multiples. En effet, ces racines sont en bijection avec les facteurs irréductibles de degrés 1. Cependant, il n'est pas satisfaisant d'un point de vue complexité de factoriser complètement un polynôme si l'on ne recherche que les facteurs d'un degré donné. La (Proposition 3.1.2) permet de résoudre simplement ce problème. En effet, on sait que le polynôme $X^p - X$ est le produit de tous les polynômes unitaires de degrés 1 :

$$X^p - X = \prod_{w \in \mathbb{F}_p} (X - w)$$

ainsi,

$$H = pgcd(X^p - X, P)$$

est égal au produit de tous les facteurs de degré 1 de P(X), et il suffit d'appliquer l'algorithme de Berlekamp sur H pour trouver les facteurs de degrés 1 (donc les racines) de P(X). Cette méthode nous donne les facteurs de degrés 1, mais qu'en est-il des facteurs irréductibles. On va maintenant voir comment généraliser cette méthode à la recherche de facteurs irréductibles de degrés fixés.

4.2.2 Distinct Degree Factorization

Plus généralement, on peut factoriser un polynôme $P \in \mathbb{F}_p[X]$ en groupes de facteurs irréductibles de même degré (distinct degree factorisation). Cette approche est basée sur la théorie des corps finis. Rappelons que tout polynôme $P(X) \in \mathbb{F}_p[X]$ irréductible de degré d définit une extension de degré d de $\mathbb{F}_p$

$$K = \frac{\mathbb{F}_p[X]}{(P(X))}$$

K est un corps fini à p^d éléments, et l'ensemble des inversibles $K^* = K \setminus \{0\}$ est un groupe multiplicatif de cardinal $p^d - 1$. Ainsi, tout élément $z \in K^*$ est racine du polynôme $X^{p^d-1} - 1$, et tout élément de K est racine du polynôme

$$Q_d = X^{p^d} - X$$

Comme Q_d a au plus p^d racines, il s'en suit que

$$K = \{z \in \overline{\mathbb{F}_p}, z^{p^d} - z = 0\}$$

ou $\overline{\mathbb{F}_p}$ désigne la clôture intégrale de $\mathbb{F}_p$. On la note $\mathbb{F}_q$ ou $q = p^d$ Comme pour le cas d= 1, on a alors l'égalité

$$X^p - X = \prod_{z \in \mathbb{F}_p} (X - z)$$

dans $\mathbb{F}_p[X]$. La proposition (3.1.2) nous donne une bonne description des polynômes irréductibles de $\mathbb{F}_p[X]$

On a $X^{p^n} - X$ est produit de facteurs irréductibles dont le degré de chaque facteurs divise n.

Premièrement regardons le cas $n = 1$. Ce cas revient au cas de la recherche des racines simples c'est à dire la recherche des facteurs de degré 1.

Posons $G_1(X) = pgcd(P(X), X^p - X)$. On obtient tous les facteurs de $P(X)$ de degré 1. Notons $P_2(X) = \dfrac{P(X)}{G_1(X)}$. Posons ensuite $G_2(X) = pgcd(P_2(X), X^{p^2} - X)$ donne les facteurs irréductibles de degré 2, on est sur qu'il n'y a plus les facteurs de degré 1, car ils ont été enlevés par la division de $\dfrac{P(X)}{G_1(X)}$. Ainsi de suite de suite en répétant le même processus on obtient les facteurs irréductibles de $P(X)$.

Mais cet algorithme a un problème, ce problème se trouve au niveau du calcul des $pgcd(P_i(X), X^{p^i} - X)$ si i est très grand.

Mais on peut dévier ce problème en calculant :

$$X^{p^i} - X \mod P_i(X) = (X^{p^i} \mod P_i(X)) - (X \mod P_i(X))$$

par la méthode de l'exponentiation rapide.

On déduit un algorithme **DistDegFact**$(\mathbf{P}, \mathbf{p})$ qui renvoie la liste des groupes de facteurs irréductibles de même degrés.

Algorithm : Distinct Degree factorization

– Donnée : $P(X) \in \mathbb{F}_p$ de Degré n

1 : $P_0 = P$
2 : Pour i=1 jusqu'à n
3 : $S_i = X^{p^i} mod P_{i-1}$ exponentiation rapide
4 : $G_i = pgcd(P_{i-1}, S_i - X)$
5 : $P_i = P_{i-1}/G_i$
6 : Fin pour
7 : $Retour\{P_1, P_2, \cdots, P_n\}$.

4.2.3 Cantor-Zassenhauss

Puisque l'on peut exprimer un polynôme sans facteur carrés comme le produit de facteurs irréductibles de même degré, il nous suffit de savoir factoriser de tels polynômes. L'approche est similaire à celle développée par Berlekamp probabiliste.

Soit donc un polynôme $P(X) \in \mathbb{F}_p[X]$ sans facteur carré comme produit de facteurs irréductibles de même degré exactement r. D'après la section précédente, on sait donc que $P(X)$ divise $X^{p^r} - X$. D'autre part, on a le lemme suivant.

LEMME 4.2.1
Pour tout $G(X) \in \mathbb{F}_p[X]$, $X^{p^r} - X$ *divise* $G(X)^{p^r} - G(X)$

Preuve

Soit $G(X) = \sum_{i=}^{n} a_i X^i$. Puisque le corps considéré est $\mathbb{F}_p[X]$, on a $G^{p^r}(X) = G(X^{p^r})$ et $G^{p^r}(X) - G(X) = G(X^{p^r}) - G(X) = \sum_{i=0}^{n} a_i(X^{ip^r} - X^i) = (X^{p^r} - X)(\sum_{i=0}^{n-1} X^{n+i(p^r-1)})$ alors $G(X)^{p^r} - G(X)$ divisible par $X^{p^r} - X$.

On écrit maintenant

$$G(X)^{p^r} - G(X) = G(X)(G(X)^{\frac{p^r-1}{2}} - 1)(G(X)^{\frac{p^r-1}{2}} + 1)$$

Ces trois facteurs étant premiers entre eux, et comme $P(X)$ divise $G(X)^{p^r} - G(X)$, on obtient la décomposition de P suivante

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

L'algorithme de Cantor-Zassenhauss consiste à tirer au sort un polynôme G de degré $< 2r$ et de vérifier si la décomposition précédente est non triviale.

Exemple

Factorisons le polynôme $P(X) = X^5 + 4X^2 + 3X + 1$ sur $\mathbb{F}_{17}$

On a $P'^4 + 8X + 3$ et $pgcd(P(X), P'(X)) = 1$ alors P(X) est sans facteur carré . Nous allons regrouper les facteurs de même degré distinct degré factorisation.

On a :

$H_1(X) = pgcd(P(X), X^{17} - X) = X^2 + 8X + 1$, ensuite on effectue $\dfrac{P(X)}{G_1(X)} = X^3 + 9X^2 + 12X + 1$, posons $P_1(X) = X^3 + 9X^2 + 12X + 1$

$H_2(X) = pgcd(P_1(X), X^{17^2} - X) = 1$, il n'y a pas de facteur irréductible de degré 2.

$H_3(X) = pgcd(P_1(X), X^{17^3} - X) = X^3 + 9X^2 + 12X + 1$.

On va maintenant casser ces groupes de facteurs, en utilisant l'algorithme de Berlekamp, on peut voir que le noyau de la matrice de Berlekamp est engendré par les vecteurs (1,0,0,0,0) et (0,-5,-8,1,0) les représentants polynômes sont $G_1(X) = 1$ et $G(X) = X^3 - 8X^2 - 5X$. Nous allons utiliser $G(X) = X^3 - 8X^2 - 5X$ pour factoriser les polynômes $H_1(X)$ et $P_1(X)$

$pgcd(H_1(X), G(X)) = 1$

$pgcd(H_1(X), G^8(X) - 1) = X - 11$

$pgcd(H_1(X), G^8(X) + 1) = X + 14$

$H_3(X) = X^3 + 9X^2 + 12X + 1$ est irréductible car il est déjà de degré 3.

finalement on obtient que :

$$P = (X + 11)(X + 14)(X^3 + 9X^2 + 12X + 1)$$

4.3 Décomposition des polynômes cyclotomiques sur un corps fini

4.3.1 Polynômes cyclotomiques irréductibles

Soit n un entier positif. Et k un corps de caractéristique 0 ou p ; où p est un nombre premier ne divisant pas n. Alors le nombre des racines n-ièmes primitives de l'unité sur k est $\varphi(n)$.
Ces $\varphi(n)$ éléments sont les générateurs de l'unique sous-groupe cyclique G_n d'ordre n de k^*, c'est le groupe des racines n-ièmes de l'unité sur k :

$$G_n = \left\{ x \in k^* \,/\, x^n = 1 \right\}.$$

Polynômes cyclotomique sur $\mathbb{C}[X]$

L'application $\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{C}^* \\ k & \mapsto & \exp^{(\frac{2i\pi k}{n})} \end{array}$ est un morphisme du groupe additif $\mathbb{Z}$ vers le groupe multiplicatif $\mathbb{C}^*$.
Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes des entiers premiers avec n, son ordre est $\varphi(n)$ où φ est la fonction d'Euler.

Les $\varphi(n)$ nombres complexes $e^{\frac{2i\pi k}{n}}$ avec $k \in (\mathbb{Z}/n\mathbb{Z})^*$ sont les racines primitives de l'unité sur $\mathbb{C}$.
Pour tout n entier positif, on défini le polynôme $\Phi_n(X) \in \mathbb{C}[X]$ par :

$$\Phi_n(X) = \prod_{\substack{k \in \{0 \cdots n-1\} \\ k \wedge n = 1}} (X - e^{\frac{2ik\pi}{n}})$$

C'est le *polynôme cyclotomique* d'indice n. Il est unitaire, de degré $\varphi(n)$.

PROPOSITION 4.3.1

Pour tout entier $n \in \mathbb{N}^*$, on a :
$X^n - 1 = \prod_{d|n} \Phi_d$

Preuve

Pour cela, nous allons prouver que les racines de l'un sont aussi celles de l'autre. Et réciproquement

. Soit α une racine de $X^n - 1$.
C'est une racine n-ieme de l'unité donc un élément du groupe multiplicative G_n. Dans ce groupe, cet élément a un ordre d c'est à dire un entier naturel tel que $\alpha^d = 1$, cette égalité fait de α une racine d-ième de l'unité donc un élément de G_d. Qui plus est, comme l'ordre de α est égal au cardinal du groupe G_d, alors il engendre celui-ci. α est une racine d-ième primitive de l'unité. Ainsi α est une racine du polynôme cyclotomique Φ_d. Mais l'histoire ne s'arrête pas la ! En fait, dans tout groupe l'ordre de chaque élément divise nécessairement le cardinal de celui-ci.
Dans le groupe G_n, l'élément α a pour ordre d. Donc $d \mid n$.
En conclusion : α est une racine du produit $\prod_{d|n} \Phi_d$.

. Soit β une racine du produit $\prod_{d|n} \Phi_d$.
Il existe un polynôme cyclotomique $\prod_{d|n} \Phi_d$ dont β est la racine. De plus $d \mid n$.
Intéressons-nous à β^n.

$$\beta^n = \beta^{d \times \frac{n}{d}} = (\beta^d)^{\frac{n}{d}} = 1$$

.
β est aussi racine polynôme $X^n - 1$. Dans $\mathbb{C}[X]$, tous les polynômes sont entièrement scindés. Le fait que deux d'entre eux aient les mêmes racines veut dire qu'ils ont le même

degré, sont associés et donc différents d'un nombre complexe. Il existe donc un nombre complexe c tel que :

$$X^n - 1 = c \prod_{d|n} \Phi_d$$

Or nos deux polynômes sont unitaires, par conséquent, le nombre complexe vaut nécessairement 1.
D'où l'égalité :

$$X^n - 1 = \prod_{d|n} \Phi_d$$

.

Ainsi de l'égalité précédente on en déduit que :

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{d|n, 1 \leq d < n} \Phi_d(X)}$$

Exemple
Calculons $\Phi_{10}(X)$
$X^{10} - 1 = \Phi_1(X)\Phi_2(X)\Phi_5(X)\Phi_{10}(X)$
On cherche les $\Phi_i(X)$?

$$\begin{aligned} X - 1 &= \Phi_1(X) \\ X^2 - 1 &= \Phi_1(X)\Phi_2(X) \implies \Phi_2(X) = X + 1 \\ X^5 - 1 &= \Phi_1(X)\Phi_5(X) \implies \Phi_5(X) = X^4 + X^3 + X^2 + X + 1 \end{aligned}$$

On obtient que :

$$\begin{aligned} \Phi_{10}(X) &= \frac{X^{10} - 1}{(X-1)(X+1)(X^4 + X^3 + X^2 + X + 1)} \\ \Phi_{10}(X) &= \frac{(X^5)^2 - 1}{(X+1)(X^5 - 1)} \\ \Phi_{10}(X) &= \frac{(X^5 + 1)(X^5 - 1)}{(X^5 - 1)(X + 1)} \\ \Phi_{10}(X) &= \frac{X^5 + 1}{X + 1} \\ \Phi_{10}(X) &= X^4 - X^3 + X^2 - X + 1 \end{aligned}$$

La liste des 55 premiers polynômes cyclotomiques est donnée en annexe a la page (52)

Pour p premier on a :

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + ... + X + 1$$

THEOREME 4.3.1 *Pour tout entier positif n, le polynôme $\Phi_n(X)$ est irréductible dans $\mathbb{Z}[X]$.*

Preuve

1. **Appartenance de Φ_n $\tilde{\mathbf{A}}$ $\mathbb{Z}[X]$.**

   Procédons par récurrence sur $n \geq 1$. $\Phi_1(X) = X - 1$ est irréductible et appartient à $\mathbb{Z}[X]$ initialise la récurrence. Soit $n \geq 2$. Par hypothèse de récurrence, $P(X) = \prod_{d|n, d\neq n} \Phi_d(X)$ est dans $\mathbb{Z}[X]$. Effectuons la division euclidienne dans $\mathbb{Z}[X]$ de $X^n - 1$ par P unitaire : $X^n - 1 = QP + R$, avec $(Q, R) \in \mathbb{Z}[X]$ et $degR < degP$. Si lâ€™on effectue maintenant la division euclidienne dans $\mathbb{C}[X]$ de $X^n - 1$ par P : $X^n - 1 = \phi_n P$. Par unicité du quotient dans la division euclidienne dans $\mathbb{C}[X]$, $\phi_n = Q \in \mathbb{Z}[X]$.

2. **Irréductibilité de Φ sur $\mathbb{Z}$**

   LEMME 4.3.1 *(Lemme de Gauss) Soit $P \in \mathbb{Z}[X]$ unitaire, et $P_1, ..., P_r \in \mathbb{Q}[X]$ unitaires tels que $P = P_1...P_r$. Alors les P_i sont tous dans $\mathbb{Z}[X]$. En particulier, P est irréductible sur $\mathbb{Z}$ si et seulement si P est irréductible sur $\mathbb{Q}$.*

   Notons U_n le groupe des racines n-èmes de l'unité dans $\mathbb{C}$, et U_n^* l'ensemble des racines n-ièmes primitives de l'unité, c'est-à -dire des générateurs de U_n. Soit $\zeta \in U_n^*$, notons μ son polynôme minimal sur $\mathbb{Q}$. μ est un diviseur unitaire irréductible de $P = X^n - 1$ sur $\mathbb{Q}$, donc d'après le lemme de Gauss, $\mu \in \mathbb{Z}[X]$. écrivons $P = \mu Q$, $Q \in \mathbb{Z}[X]$. Soit p premier ne divisant pas n. D'après le lemme de Frobenius on a $\mu(X^p) - (\mu(X))^p = pR(X)$, avec $R \in \mathbb{Z}[X]$.
   En évaluant en ζ, on obtient $\mu(\zeta^p) = pR(\zeta)$. Montrons que $\mu(\zeta^p) = 0$: raisonnons par l'absurde et supposons $\mu(\zeta^p) = 0$. Comme $P(\zeta^p) = 0$, alors $Q(\zeta^p) = 0$. En dérivant $P = \mu Q$ et en évaluant en ζ^p, on obtient $n(\zeta^p)^{n-1} = \mu(\zeta^p)Q'(\zeta^p) = pR(\zeta)Q'(\zeta^p)$. En multipliant les deux membres par ζ^p, il vient : $n = pT(\zeta)$, où $T(X) = X^p R(X)Q'(X^p) \in \mathbb{Z}[X]$. Notons d le degré de μ. En appelant $U \in \mathbb{Z}[X]$ le reste dans la division euclidienne de T par μ unitaire dans $\mathbb{Z}[X]$, on a même $n = pU(\zeta) = p(\sum_{k=0}^{d-1} a_k \zeta^k$, avec les a_k dans $\mathbb{Z}$. Or, $(1, \zeta, ..., \zeta^{d-1})$ est libre sur $\mathbb{Q}$, donc par unicité de lâ€™écriture de n dans cette base, $n = p \ \ a_0, a_0 \in \mathbb{Z}$, ce qui est absurde, car p ne divise pas n. Dâ€™où $\mu(\zeta^p) = 0$. μ est donc aussi le polynôme minimal de ζ^p sur $\mathbb{Q}$. On en déduit par récurrence que si m est premier avec n, ζ^m est aussi racine de μ, soit que tout élément de U_n^* est racine de μ.

   Donc Φ_n unitaire non constant divise μ unitaire irréductible : $\Phi_n = \mu$ est le polynôme minimal de ζ, donc irréductible.

PROPOSITION 4.3.2
Soit K un corps et $n \in \mathbb{N}^*$. Supposons que K soit de caractéristique un nombre p premier, tel que p soit premier avec n. Alors le polynôme $\Phi_n(X)$ est séparable sur K et ses racines sont exactement les racines n-ièmes primitives de l'unité sur K

Preuve

La dérivée du polynôme $X^n - 1$ est nX^{n-1} dans K et $pgcd(X^n - 1, nX^{n-1}) = 1$ d'où $X^n - 1$ est séparable sur K,puisque $\Phi_n(X)$ est un facteur de $X^n - 1$ par conséquent $\Phi_n(X)$ est aussi séparable sur K. Les racines de $X^n - 1$ sur K sont précisément les n-ièmes racines de l'unité contenues dans K. Une racine n-ièmes de l'unité est primitive si et seulement si elle n'est pas racine de ϕ_d lorsque $d \mid n$ et $d \neq n$. Cela veut dire qu'elle est racine de ϕ_n.

Si $n = mp^r$ avec $r \geq 0$ et $m \geq 1$, en caractéristique p on a :
$X^n - 1 = (X^m - 1)^{p^r}$
D'où, si p divise n il n'y a pas de racines primitive n-ième de l'unité dans un corps de caractéristique p.

4.3.2 Polynômes cyclotomiques sur un corps fini

Soit $n \in \mathbb{N}^*$ et p un nombre premier tel que $pgcd(p,n)' = 1$
Rappelons l'écriture de $\Phi_{n,\mathbb{F}_p}$ sur $\mathbb{F}_p$. On a :

$$\Phi_{n,\mathbb{F}_p}(X) = \prod_{\omega \in \Omega_n} (X - w) \qquad (**)$$

ou Ω_n désigne l'ensemble des $\varphi(n)$ racines n-ièmes primitives de l'unité sur $\mathbb{F}_p$.

4.3.3 Condition d'irréductibilité des polynômes cyclotomiques sur $\mathbb{F}_p$

THEOREME 4.3.2
Soit ω une racine n-ième primitive de l'unité sur $\mathbb{F}_p$, et m un entier naturel non nul.

a) Si $deg(Irr_{\mathbb{F}_p,\omega}(X)) = m$, alors m ne dépend du choix de la racine n -ième primitive de lunité et on a :

b) $\Phi_{n,\mathbb{F}_p}(X) \in \mathbb{F}_p[X]$ se décompose en produit de $k = \frac{\varphi(n)}{m}$, polynômes irréductibles sur $\mathbb{F}_p$

c) m est l'ordre de $\overline{p}$ dans $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$.

d) $\Phi_{n,\mathbb{F}_p}$ est irréductible sur $\mathbb{F}_p \Longleftrightarrow k = 1 \Longleftrightarrow m = \varphi(n) \Longleftrightarrow \overline{p}$ engendre $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$

Preuve

Etape 1 : Montrons d'abord que si $\omega \neq \omega'$ sont deux racines n-ièmes primitive de l'unité alors :

$$deg(Irr_{\mathbb{F}_p,\omega}(X)) = deg(Irr_{\mathbb{F}_p,\omega'}(X))$$

Par définition du polynômes minimal associe à un élément on a :

$deg(Irr_{\mathbb{F}_p,\omega}(X)) = [\mathbb{F}_p(\omega) : \mathbb{F}_p]$ et $deg(Irr_{\mathbb{F}_p,\omega'}(X)) = [\mathbb{F}_p(\omega') : \mathbb{F}_p]$

Comme ω est une racine n-ième primitive de l'unité, elle engendre $\mathbb{U}_{n,\mathbb{F}_p}$ le groupe des racines n-ième de l'unité sur $\mathbb{F}_p$ et il existe donc $k \in \overline{1 : n-1}$, $\omega'^k \Longrightarrow \omega' \in \mathbb{F}_p(\omega) \Longrightarrow \mathbb{F}_p(\omega') \subset \mathbb{F}_p(\omega)$ Pour les mêmes raisons, on a également l'inclusion $\mathbb{F}_p(\omega) \subset \mathbb{F}_p(\omega')$ soit :

$$\mathbb{F}_p(\omega) = \mathbb{F}_p(\omega')$$

Notons alors $m = deg(Irr_{\mathbb{F}_p,\omega}(X)) \in \mathbb{N}^*$ qui est donc d après ce qui précède, indépendant du choix de la racine n- ieme primitive de l'unité.

Etape 2 . Montrons que $\Phi_{n,\mathbb{F}_p}(X) \in \mathbb{F}_p[X]$ est un produit de $\frac{\varphi(n)}{m}$ polynômes minimaux de racines n-iemes primitives de l'unité. Rappelons l'écriture de $\Phi_{n,\mathbb{F}_p}(X)$, on a

$$\Phi_{n,\mathbb{F}_p}(X) = \prod_{\omega \in \Omega_n} (X - w) \qquad (**)$$

ou Ω_n désigne l'ensemble des $\varphi(n)$ racines n-ièmes primitives de l'unité sur $\mathbb{F}_p$. Considérons $P(X)$ un polynômes qui est un facteur irréductibles unitaire sur $\mathbb{F}_p$ de $\Phi_{n,\mathbb{F}_p}(X)$, d'après $(**)$ on a en particulier :

$$\exists \omega \in \Omega_n, P(\omega) = 0 \Longrightarrow Irr_{\mathbb{F}_p,\omega}(X) \mid P(X)$$

Or, P lui aussi est irréductible et unitaire sur $\mathbb{F}_p$, on en déduit que

$$P(X) = Irr_{\mathbb{F}_p,\omega}(X), deg(Irr_{\mathbb{F}_p,\omega}(X)) = deg(P(X)) = m$$

Comme $\Phi_{n,\mathbb{F}_p}(X)$ est scindé simples dans son corps de décomposition (**), nécessairement $\Phi_{n,\mathbb{F}_p}(X)$ est sans facteur multiple sur $\mathbb{F}_p$ et s'écrit comme un produit de polynômes minimaux deux à deux distincts : $\Phi_{n,\mathbb{F}_p}(X) = \prod_{i=1}^{k} Irr_{\mathbb{F}_p,\omega_i}(X)$ ou $deg(Irr_{\mathbb{F}_p,\omega_i}(X)) = m$ pour tout $\in \overline{1:k}$ et donc $deg(\Phi_{n,\mathbb{F}_p}(X)) = \varphi(n) = \sum_{i=1}^{k} deg(Irr_{\mathbb{F}_p,\omega_i}(X)) = km$.

Conclusion $\Phi_{n,\mathbb{F}_p}(X))$ est donc produit de $\frac{\varphi(n)}{m}$ polynômes irréductibles sur $\mathbb{F}_p$ et $\phi_{n,\mathbb{F}_p}(X))$ est irréductibles sur $\mathbb{F}_p$ si et seulement si $k = 1 \Longleftrightarrow m = \varphi(n)$

Etape 3 : Montrons que m est l'ordre de $\overline{p}$ dans $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$. D' après ce qui précède on a :

. $\omega^n = 1$ car ω est racine n-ième de primitive de l'unité.
. $[\mathbb{F}_p(\omega) : \mathbb{F}_p] = deg(Irr_{\mathbb{F}_p,\omega}(X)) = m$.
. $\mathbb{F}_p(\omega) \simeq \mathbb{F}_p^m$ est $card(\mathbb{F}_p(\omega)) = p^m \Longrightarrow card(\mathbb{F}_p(\omega)^*) = p^m - 1$
Comme $\omega \in \mathbb{F}_p(\omega)^*$ et est d'ordre n, on en déduit que : $\omega^{p^m-1} = 1 \Longrightarrow n \mid p^m - 1 \Longleftrightarrow p^m \equiv 1[n]$

LEMME 4.3.2 *Soit $P(X) = X^n + \cdots + a_1X \pm 1 \in \mathbb{Z}[X]$, non constant. Alors, il existe une infinité de nombres premiers p tels que $\overline{P}$ la réduction modulo p de $P(X)$ ait une racine dans $\mathbb{F}_p$.*

Preuve

Supposons par l'absurde qu'il y ait un nombre fini de nombres premiers, $p_1, \cdots, p_r \in \mathcal{P}$ pour lesquels réduit modulo p_i, $\overline{P}$ ait des racines dans $\mathbb{F}_{p_i}$. On note $M = \prod_{i=1}^{r} p_i > 0$.

Méthode : Considérons $G(X) = P(MX)$ et montrons qu il existe $x \in \mathbb{Z}$ tel que $G(x) \neq 0, -1, 1$. Pour ce faire, il suffit de montrer qu'il existe un $x \in \mathbb{Z}$ qui n'est pas racine de $G(X)$ de $G(X) - 1$, et $G(X) + 1$. Comme $G(X)$ est non constant, ces 3 polynômes n'admettent qu'un nombre fini de racines et $\mathbb{Z}$ étant infini, il existe $x \in \mathbb{Z}$ qui ne soit racine d aucun des 3 polynômes et donc tel que $G(x) \neq 0, 1, -1$. Pour un tel x, on a $G(x) \in \mathbb{Z}$ et donc $\mid G(x) \mid \geq 2$ et donc $G(x)$ admet donc un diviseur premier, que l'on note q. Ainsi,

$q \mid G(x) = P(Mx) = \pm 1 + a_1Mx + \cdots + (Mx)^n \Longrightarrow \overline{G(x)} = 0 = \overline{P(Mx)}$ dans $\mathbb{F}_q$ $(\circ)$. On en déduit que donc que $\overline{Mx}$ est racine de $\overline{P}$ dans $\mathbb{F}_q$, ce qui d'après nos hypothèse donne :

$\exists \in \overline{1:r}$ tel que $q = p_i$ et en particulier $q \mid M = \prod_{i=1}^{k} p_i$.

Dans $\mathbb{F}_q$, on a alors :
$\overline{P(Mx)} = 1 + \overline{a_1Mx} + \cdots + \overline{(a_nMx)^n} = \overline{1}$ car $q \mid M$ et $\overline{P(Mx)} \neq 0$

En contradiction avec $(\circ)$. Ainsi il ya une infinité de nombre premiers p tel que la réduction de P(X) modulo p, ait des racines dans $\mathbb{F}_p$.

Nous remarquons que à partir du lemme(4.3.3) précédent certains polynômes cyclotomiques sont réductibles sur les corps finis. Dans la partie suivant nous allons voir comment décomposer un polynôme cyclotomique sur un corps finis.

4.4 Décompositions de polynômes cyclotomiques sur un corps fini

Soient le corps $\mathbb{F}_q$ de caractéristique q et $n \in \mathbb{N}$. Si q ne divise pas n, alors le polynôme cyclotomique ϕ_n est séparable sur $\mathbb{F}_q$. En effet, si ϕ_n admet un zéro multiple, il en est de même de $X^n - 1 \in \mathbb{F}_q[X]$ ce qui signifie que $nX^{n-1} \equiv 0$ dans $\mathbb{F}_q$ donc $n \equiv 0 \mod p$.
Ainsi, dans $\mathbb{F}_5[X]$, le polynôme $\phi_{12}(X)$ n'est pas irréductible

$$\phi_{12}(X) = X^4 - X^2 + 1 = (X^2 - 2X - 1)(X^2 + 2X - 1)$$

Dans toute cette section, on suppose que n n'est pas divisible par la caractéristique q de $\mathbb{F}_q$.

THEOREME 4.4.1 *Soit $\mathbb{F}_q$ un corps fini à q éléments et $n \in \mathbb{N}^*$. Alors le polynôme cyclotomique Φ_n se décompose sur $\mathbb{F}_q$ en un produit de $\frac{\varphi(n)}{d}$ facteurs irréductibles, tous de même degré d'où d est l'ordre de q modulo n.*

Preuve

Soit ζ une racine primitive de ϕ_n dans le corps de décomposition de K du polynôme ϕ_n. sur $\mathbb{F}_q$. L'ordre de ζ dans le groupe multiplicatif K^* est n. Le degré de ζ sur $\mathbb{F}_q$ est le plus petit entier $s \geq 1$ tel que $\zeta^{q^s-1} = 1$. D'ou c'est le plus petit entier positif tel que n divise $q^s - 1$ et c'est l'ordre de q dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

Classes cyclotomiques

Soit $n = p^m$, les classes cyclotomiques permettent de décomposer en facteurs irréductibles le polynôme : $X^{p^m-1} - 1$ sur $\mathbb{F}_p[X]$. Ainsi on aura le nombre de facteurs irréductibles de $\Phi_{p^m-1}(X)$. Elles permettent de trouver tous les facteurs irréductibles de $X^{p^m-1} - 1$ sur $\mathbb{F}_p$.

Remarquons que si $p^m - 1$ est premier alors $X^{p^m-1} - 1 = \Phi_{p^m-1}(X)$.

En effet dans, $\mathbb{C}$: $\Phi_n(X) = \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^*} (X - \exp^{(\frac{2i\Pi k}{n})}) = \dfrac{X^n - 1}{\prod_{d|n,1\leq d<n} \Phi_d(X)} \Leftrightarrow X^n - 1 = \prod_{d|n} \Phi_d(X)$

On utilise le premier théorème de mobiüs sous forme multiplicative, on obtient : $\Phi_n(X) = \prod_{d//n} (X^d - 1)^{\mu(n/d)}$

Donc dans un corps fini on a : $X^{p^m-1} - 1 = \prod_{d|p^m-1} \Phi_d(X)$. Et $\Phi_d(X) = \prod_{s\in(\mathbb{Z}/d\mathbb{Z})^*} (X - \alpha^s) = \prod_{\ell//p^m-1} (X^\ell - 1)^{\mu(d/\ell)}$

Revenons à la décomposition de $\Phi_{p^m-1}[X]$

DEFINITION 4.4.1 *On appelle classe cyclotomique p-aire modulo $n-1 = p^m - 1$, de l'entier i, l'ensemble des entiers modulo $n-1$ de la forme ip^j pour $0 \leq i \leq p^m - 1$ et $0 \leq j \leq m_s - 1, m_s = min\{j : ip^j \equiv i[p^m - 1]\}$ on note*
$C_i = \left\{i, ip, ip^2, ..., ip^{m_i-1}\right\}$ la classe cyclotomique de i modulo $p^m - 1$. Elle contient l'entier i, et m_i est le plus petit entier positif tel que :
$iq^{m_i} \equiv i \mod n$.

Il existe une correspondance bijective entre les facteurs irréductibles de $X^{p^m-1} - 1$ et les classes cyclotomiques p-aires module $p^m - 1$. En particulier, le nombre de facteurs irréductibles de $X^{p^m-1} - 1$ est égal au nombre de classes cyclotomiques. Le degré d'un facteur irréductible est égal au cardinal de la classe cyclotomique associée. L'entier i est souvent appelé chef de classe ou coset leader en anglais.

Exemple

On se place sur le corps fini de caractéristique 2 et longueur 3, c'est-à -dire, sur le corps $\mathbb{F}_{2^3}$.

On veut construire les classes cyclotomiques 2-aire modulo $2^3 - 1 = 7$ de telle sorte que l'on puisse décomposer $X^{2^3-1} - 1 = X^7 - 1 = \phi_7[X]$

Pour $i = 0$

$j \leq 7$, $0 \times 2^1 = 0 \bmod 7 = 0$

Alors $C_0 = 0$

Pour $i = 1$

$j = 0, 2^0 \times 1 = 1 \mod 7 = 1$

$j = 1, 2^1 \times 1 = 2 \mod 7 = 2$

$j = 2, 2^2 \times 1 = 4 \mod 7 = 4$

$j = 3,\ 2^3 \times 1 = 8 \mod 7 = 1 \Rightarrow m_1 = 3.$
Alors $C_1 = \{2, 4, 1\}$

Pour $i = 2$

$j = 0, 2^0 \times 2 = 2 \mod 7 = 2$

$j = 1, 2^1 \times 2 = 4 \mod 7 = 4$

$j = 2, 2^2 \times 2 = 8 \mod 7 = 1$

Alors $C_2 = \{4, 1, 2\}$

Pour $i = 3$

$j = 0, 2^0 \times 3 = 3 \mod 7 = 3$

$j = 1, 2^1 \times 3 = 6 \mod 7 = 6$

$j = 2, 2^2 \times 3 = 12 \mod 7 = 5$

Alors $C_3 = \{6, 5, 3\}$

Finalement, on a :

$C_0 = \{0\}$

$C_1 = C_2 = C_4 = \{1, 2, 4\}$

$C_3 = C_5 = \{3, 5, 6\}$

Avec les classes cyclotomiques, nous pouvons trouver les facteurs irréductibles de $\Phi_{p^m-1}[X]$ sur $\mathbb{F}_p[X]$. On a :

$$\Phi_{p^m-1}[X] = \frac{X^{p^m-1} - 1}{\prod_{d|_{p^m-1}, 1 \leq d < p^m-1} \Phi_d(X)} \quad \text{où } \Phi_d(X) = \prod_{i \in C_i} (X - \alpha^i)\,;$$

tel que $m_i \in C_i$ est le plus petit entier tel que $ip^{m_i} \equiv i \mod (p^m - 1)$ et $d \mid p^m - 1$ et d est tel que $(\alpha^i)^d = 1$ α étant l'une des racines primitives du polynôme $X^{p^m-1} - 1$.
Déterminons la décomposition des polynômes cyclotomiques $\phi_7(X)$ et $\phi_{15}(X)$ sur $\mathbb{F}_2[X]$.

Décomposition du polynôme cyclotomique $\phi_7(X)$ sur $\mathbb{F}_2[X]$

D'abord, on cherche les classes cyclotomiques C_i en suivant la procédure décrite ci-dessus. Pour $2^3 - 1$ sur $\mathbb{F}_{2^3}$, on a les classes cyclotomiques suivantes :

$C_0 = \{0\}$
$C_1 = C_2 = C_4 = \{1, 2, 4\}$
$C_3 = C_5 = \{3, 5, 6\}$

A l'aide de la table des éléments du corps $\mathbb{F}_{2^3}$ ci-dessus, on construit les polynômes irréductibles de $\Phi_7(X)$ sur $\mathbb{F}_{2^3}$.

$$\begin{aligned}
\Phi_7(X) &= [(X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^3)(X-\alpha^6)(X-\alpha^5)] \\
&= [(X^2+\alpha X+\alpha^2 X+\alpha^3)(X-\alpha^4)(X^2+\alpha^6 X+\alpha^3 X+\alpha^9)(X-\alpha^5)] \\
&= [(X^3+\alpha X^2+\alpha^2 X^2+\alpha^3 X+\alpha^4 X^2+\alpha^5 X+\alpha^6 X+\alpha^7)]\times \\
&\quad [(X^3+\alpha^6 X+\alpha^3 X^2+\alpha^9 X+\alpha^5 X^2+\alpha^{11} X+\alpha^8 X+\alpha^{14})] \\
&= [(X^3+(\alpha+\alpha^2+\alpha^4)X^2+(\alpha^3+\alpha^5+\alpha^6)X+\alpha^7)]\times \\
&\quad [(X^3+(\alpha^6+\alpha^3+\alpha^5)X^2+(\alpha^9+\alpha^{11}+\alpha^8)X+\alpha^{14})]
\end{aligned}$$

La table ci-dessus montre les éléments du corps $\mathbb{F}_{2^3}$ avec $P(X) = X^3 + X + 1$

Puissance de α	les éléments de $\mathbb{F}_{2^3}$	Polynôme	α^2	α	1
0	1	1	0	0	1
1	α	α	0	1	0
2	α^2	α^2	1	0	0
3	α^3	$\alpha+1$	0	1	1
4	α^4	$\alpha^2+\alpha$	1	1	0
5	α^5	$\alpha^2+\alpha+1$	1	1	1
6	α^6	α^2+1	1	0	1

D'après la tables des éléments de $\mathbb{F}_{2^3}$ on a :

$$\begin{aligned}
\alpha+\alpha^2+\alpha^4 &= \alpha+\alpha^2+\alpha+\alpha^2 \\
&= 2\alpha^2+2\alpha \\
&= 0 \\
\alpha^3+\alpha^5+\alpha^6 &= \alpha+1+\alpha^2+\alpha+1+\alpha^2+1 \\
&= 2\alpha^2+2\alpha+2+1 \\
&= 1 \\
\alpha^7 &= \alpha\alpha^6 = \alpha(\alpha^2+1) \\
&= \alpha^3+\alpha = \alpha+1+\alpha \\
&= 2\alpha+1 = 1 \\
\alpha^9+\alpha^{11}+\alpha^8 &= (\alpha^3)^3+(\alpha^3)^3\alpha^2+\alpha^6\alpha^2 \\
&= (\alpha+1)(\alpha+1)^2+(\alpha+1)(\alpha+1)^2\alpha^2+(\alpha^2+1)\alpha^2 \\
&= (\alpha+1)(\alpha^2+1)+(\alpha+1)(\alpha^2+\alpha)\alpha^2+\alpha++\alpha^2 \\
&= (\alpha+1)(\alpha^2+1)+\alpha(\alpha+1)+\alpha \\
&= \alpha+1+\alpha+\alpha^2+1+\alpha^2+\alpha+\alpha \\
&= 1 \\
\alpha^{14} &= (\alpha^3)^2(\alpha^3)^2\alpha^2 \\
&= (\alpha+1)^2(\alpha+1)^2\alpha^2 \\
&= (\alpha^2+1)^2\alpha^2 = (\alpha^4+1)\alpha^2 \\
&= \alpha^4+\alpha^2 = \alpha^2+\alpha^2+1 \\
&= 1
\end{aligned}$$

On obtient donc :

$$\begin{aligned}
\phi_7(X) &= (X^3+\underbrace{(\alpha+\alpha^2+\alpha^4)}_{=0}X^2+\underbrace{(\alpha^3+\alpha^5+\alpha^6)}_{=1}X+\underbrace{\alpha^7}_{=1})\times \\
&\quad (X^3+\underbrace{(\alpha^6+\alpha^3+\alpha^5)}_{=1}X^2+\underbrace{(\alpha^9+\alpha^{11}+\alpha^8)}_{=0}X+\underbrace{\alpha^{14}}_{=1}) \\
\phi_7(X) &= (X^3+X+1)(X^3+X^2+1) \\
&= X^6+X^5+X^4+X^3+X^2+X+1
\end{aligned}$$

4.4.1 Application de l'algorithme de Berlekamp à la décomposition de $\Phi_7(X)$ sur $\mathbb{F}_2$

$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$, la dérivée de $\Phi_7(X)$ est $\Phi_7'(X) = 6X^5 + 5X^4 + 4X^3 + 3X^2 + 2X + 1$, et le $pgcd(\Phi_7(X), \Phi_7'(X)) = 1$ par conséquent $\Phi_7(X)$ est sans facteur multiple
Intéressons-nous à l'algèbre
$A = \dfrac{\mathbb{F}_2[X]}{(\Phi_7(X))}$ c'est $\mathbb{F}_2$-ev de dimension 6 dont une base est $\{1, X, X^2, X^3, X^4, X^6\}$. Déterminons la matrice de l'endomorphisme $F - Id$. On aura besoin des puissances $X^{2i} \mod \Phi_7(X)$ pour $0 \leq i \leq 3$

$$
\begin{aligned}
X^0 &\equiv 1 \mod \Phi_7(X) \\
X^2 &\equiv X^2 \mod \Phi_7(X) \\
X^4 &\equiv X^4 \mod \Phi_7(X) \\
X^6 &\equiv X^5 + X^4 + X^3 + X^2 + X + 1 \mod \Phi_7(X) \\
X^8 &\equiv X \mod \Phi_7(X) \\
X^{10} &\equiv X^3 \mod \Phi_7(X)
\end{aligned}
$$

$$
\begin{aligned}
(F - Id)(1) &= 1^2 - 1 \\
(F - Id)(X) &= X^2 + X \\
(F - Id)(X^2) &= X^4 + X^2 \\
(F - Id)(X^3) &= X^5 + X^4 + X^2 + X + 1 \\
(F - Id)(X^4) &= X^4 + X \\
(F - Id)(X^5) &= X^5 + X^3
\end{aligned}
$$

La matrice de l'endomorphisme est :

$$
M = \begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1
\end{pmatrix}
$$

Le rang de la matrice est exactement r=4 par conséquent P(X) à deux facteurs irréductibles distinct car $dim(A^{\mathcal{F}}) = 6 - 4$.
Pour les polynômes cyclotomiques le degré des facteurs peuvent être connus d'avance on aura $d = \dfrac{\varphi(7)}{dim(A^{\mathcal{F}})}$ c'est à dire $d = \dfrac{\varphi(7)}{2} = 3$.
Le noyau de cette matrice est engendré par deux vecteurs qui sont (1,0,0,0,0,0) et (0,1,1,0,1,0), les représentants polynômes sont $G_1(X) = 1$ et $G_2(X) = X^4 + X^2 + X$
On a :

$$pgcd(\Phi_7(X), G_2(X) = X^3 + X + 1$$
$$pgcd(\Phi_7(X), G_2(X) - 1) = X^3 + X^2 + 1$$

$\Phi_7(X) = (X^3 + X + 1)(X^3 + X^2 + 1)$

Décomposition du polynôme cyclotomique $\phi_{15}(X)$ sur $\mathbb{F}_{2^4}[X]$

De façon similaire, on cherche les classes cyclotomiques C_i en suivant la procédure décrite ci-dessus. Pour $2^4 - 1$ sur $\mathbb{F}_{2^4}$, on a les classes cyclotomiques suivantes :

Décomposons : $X^{15} - 1$
$C_0 = \{0\}$

$C_1 = \{1, 2, 4, 8\}$

$C_3 = \{3, 6, 12, 9\}$
$C_5 = \{5, 10\}$

$C_7 = \{7, 11, 13, 14\}$
D'après la tables des éléments de $\mathbb{F}_{2^4}$ on a :

$$\begin{aligned} \phi_{15}(X) &= (X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8)(X-\alpha^7)(X-\alpha^{11})(X-\alpha^{13})(X-\alpha^{14}) \\ &= (X^4 + X + 1)(X^4 + X^3 + 1) \\ &= X^8 - X^7 + X^5 - X^4 + X^3 - X + 1 \end{aligned}$$

Factorisation de $X^n - 1$ dans un corps fini $\mathbb{F}_q[X]$

Les polynômes $X^n - 1$ sur $\mathbb{F}_q[X]$ sont à la base de la construction des codes linéaires cycliques.
Supposons que $pgcd(n, q) = 1$ nous avons étudié plus haut la décomposition des polynômes cyclotomiques sur $\mathbb{F}_q$ et $X^n - 1$ est produit des $\Phi_d(X)$ pour d divisant n.
En effet toute racine primitive d'ordre d est une racine n-ième si d divise n.
Notons S_d l'ensemble des racines n-ièmes de l'unité d'ordre d. Alors $\{S_d; d \mid n\}$ est une partition de $\mu_n(\mathbb{F}_q)$ donc :

$$\prod_{\alpha^i \in \mu_n(\mathbb{F}_q)} (X - \alpha)^i) = \prod_{d|n} \prod_{\alpha^i \in S_d} (X - \alpha^i).$$

et finalement :

$$X^n - 1 = \prod_{d|n} \phi_d(X)$$

Une factorisation du polynôme $X^n - 1$ dans un corps fini $F_q[X]$ est donc entièrement déterminée par la factorisation des $\phi_d(X)$ tel que d divise n sur $\mathbb{F}_q[X]$

EXEMPLE 1 *Prenons $n = 15, q = 2$. Déterminons la décomposition de $X^{15} - 1$ sur $\mathbb{F}_2[X]$*

$$\begin{aligned} X^{15} - 1 &= \prod_{d|15} \phi_d(X) \\ &= \phi_1(X)\phi_3(X)\phi_5(X)\phi_{15}(X) \end{aligned}$$

Avec

$$
\begin{aligned}
\phi_1(X) &= (X-\alpha^0) \\
&= X+1 \\
\phi_3(X) &= (X-\alpha^5)(X-\alpha^{10}) \\
&= X^2+X+1 \\
\phi_5(X) &= (X-\alpha^3)(X-\alpha^6)(X-\alpha^9)(X-\alpha^{12}) \\
&= X^4+X^3+X+1 \\
\phi_{15}(X) &= (X-\alpha)(X-\alpha^2)(X-\alpha^4)(X-\alpha^8)\times \\
&\quad (X-\alpha^7)(X-\alpha^{11})(X-\alpha^{13})(X-\alpha^{14})
\end{aligned}
$$

d'où

$$
\begin{aligned}
X^{15}-1 &= (X-1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^4+X+1) \\
&\quad \times(X^4+X^3+1).
\end{aligned}
$$

4.5 Conclusion

Au terme de ce cours nous sommes parvenus à factoriser sur un corps fini un polynôme donné quelconque, grà⁄ce à l'algorithme de **Berlekamp**, qui historiquement et théoriquement est le premier algorithme à s'exécuter en temps polynomial, cet algorithme s'avère très efficace pour la factorisation des polynômes sur les corps finis de petite taille. Pour la factorisation des polynômes sur les corps finis de grande taille nous avons présenté l'algorithme de **Cantor-Zassenhauss** qui est très rapide et essentiellement basé sur la théorie des corps finis.

Cependant ne serai- il pas possible de trouver d'autres algorithmes plus rapides et efficaces basés sur d'autres branches telles que la géométrie algébrique, géométrie diophantienne etc. Et mieux encore donner des algorithmes qui permettent de factoriser les polynômes sur n'importe quel corps ou même sur n'importe quel anneau. Dans nos travaux futurs nous essayerons d'explorer ces différentes pistes mentionnées.

ANNEXE A

Liste des 55 premiers polynômes cyclotomiques

$$\Phi_1(X) = X - 1$$
$$\Phi_2(X) = \frac{X^2 - 1}{X - 1} = X + 1$$
$$\Phi_3(X) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1$$
$$\Phi_4(X) = \frac{X^4 - 1}{x^2 - 1} = X^2 + 1$$
$$\Phi_5(X) = X^5 + X^3 + X + 1$$
$$\Phi_6(X) = X^2 + -X + 1$$
$$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$
$$\Phi_8(X) = X^4 + 1$$
$$\Phi_9(X) = X^6 + X^3 + 1$$
$$\Phi_{10}(X) = X^4 - X^3 + X - X + 1$$
$$\Phi_{11}(X) = X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$
$$\Phi_{12}(X) = X^4 - X^2 + 1$$
$$\Phi_{13}(X) = X^{12} + X^{11} + X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$
$$\Phi_{14}(X) = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$$
$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 - X^3 - X + 1$$
$$\Phi_{16}(X) = X^8 - 1$$
$$\Phi_{17}(X) = \sum_{i=0}^{16} X^i$$
$$\Phi_{18}(X) = X^6 - X^3 + 1$$
$$\Phi_{19}(X) = \sum_{i=0}^{18} X^i$$
$$\Phi_{20}(X) = X^8 - X^6 + X^4 - X^2 + 1$$
$$\Phi_{21}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1$$
$$\Phi_{22}(X) = X^{10} - X^9 + X^8 - X^7 + X^6 - X^5 + X^4 - X^3 - X^2 - X + 1$$
$$\Phi_{23}(X) = \sum_{i=0}^{22} X^i$$
$$\Phi_{24}(X) = X^8 - X^4 + 1$$
$$\Phi_{25}(X) = X^{20} + X^{15} + X^{10} + X^5 + 1$$
$$\Phi_{26}(X) = X^{12} - X^{11} + X^{10} - X^9 + X^8 - X^7 + X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$$
$$\Phi_{27}(X) = X^{18} + X^9 + 1$$
$$\Phi_{28}(X) = X^{12} - X^{10} + X^8 - X^6 + X^4 - X^2 + 1$$

$$\Phi_{36}(X) = X^{12} - X^6 + 1$$
$$\Phi_{37}(X) = \sum_{i=0}^{36} X^i$$
$$\Phi_{38}(X) = X^{18} - X^{17} + X^{16} - X^{15} + X^{14} - X^{13} + X^{12} - X^{11} + X^{10} - X^9 + X^8 - X^7 + X^6 - X^5 + X^4 -$$
$$\Phi_{39}(X) = X^{24} - X^{23} + X^{21} - X^{20} + X^{18} - X^{17} + X^{15} - X^{14} + X^{12} - X^{10} + X^9 - X^7 + X^6 + X^4 + X^3 -$$
$$\Phi_{40}(X) = X^{16} - X^{12} + X^8 - X^4 + 1$$
$$\Phi_{41}(X) = \sum_{i=0}^{40} X^i$$
$$\Phi_{42}(X) = X^{12} + X^{11} - X^9 + X^8 + X^6 - X^4 - X^3 + X + 1$$
$$\Phi_{43}(X) = \sum_{i=0}^{42} X^i$$
$$\Phi_{44}(X) = X^{20} - X^{18} + X^{16} - X^{14} + X^{12} - X^{10} + X^8 - X^6 + X^4 - X^2 + 1$$
$$\Phi_{45}(X) = X^{24} - X^{21} + X^{15} - X^{12} + X^9 - X^3 + 1$$
$$\Phi_{46}(X) = \sum_{i=0}^{22} (-X)^i$$
$$\Phi_{47}(X) = \sum_{i=0}^{46} X^i$$
$$\Phi_{48}(X) = X^{16} - X^8 + 1$$
$$\Phi_{49}(X) = X^{49} + X^{35} + X^{28} + X^{21} + X^{14} + X^7 + 1$$
$$\Phi_{50}(X) = X^{20} - X^{15} + X^{10} - X^5 + 1$$
$$\Phi_{51}(X) = X^{32} - X^{31} + X^{29} - X^{28} + X^{26} - X^{25} + X^{23} - X^{22} + X^{20} - X^{19} + X^{17} - X^{16} + X^{15} - X^{13} + X$$
$$\Phi_{52}(X) = X^{24} - X^{22} + X^{20} - X^{18} + X^{16} - X^{14} + X^{12} - X^{10} + X^8 - X^6 + X^4 - X^2 + 1$$
$$\Phi_{53}(X) = \sum_{i=0}^{52} X^i$$
$$\Phi_{54}(X) = X^{18} - X^9 + 1$$
$$\Phi_{55}(X) = X^{40} - X^{39} + X^{35} - X^{34} + X^{30} - X^{28} + X^{25} - X^{23} + X^{20} - X^{17} + X^{15} - X^{12} + X^{10} - X^6 + X^$$

Bibliographie

[1] Michel Demazure.cours d'algèbre.Cassini, 2009.

[2] Marc Hindry. Arithmétique.calvage & Mounet,2008.

[3] J. Querré, Cours d'Algèbre, Maitrise de mathématiques,Masson, 1976.

[4] Michael Rabin. Probabilistic Algorithms in Finite Fields. SIAM J Computing 9(2)273-280,1980.

[5] [Per96] Daniel Perrin. Cours d'algèbre.

[6] R & H.Niederreiter,Finite Fields, Encyclopedia of Mathematics and Its Applications,Vol.20, Addison-weysley Publishing Company,1983

[7] [Ser70] Jean pierre Serre. Cours d'algèbre. puf,1970.

[8] Vincent Beck, Jérome Malick, and Gabriel Peyré.Objectif agregation.H&K, 2005.

[9] Gilles Zemor, cours de cryptographie.Cassini, 2000.