Cours préparatoire "Ecole sur les Codes Correcteurs d'Erreurs" (Algérie)

Corps finis

Dr. Joël KABORE

Laboratoire de Mathématiques et Informatique (LAMI)
Université Joseph KI-ZERBO
Burkina-Faso

Septembre 2025

Objectifs

- Connaitre les propriétés basiques sur les corps finis
- Construire des corps finis
- Factoriser le polynôme $X^n - 1$

Structure d'anneaux

On dit que $(A, +, .)$ est un anneau si

- $(A, +)$ est un groupe commutatif ;
- . est une loi de composition interne associative et distributive par rapport à la loi $+$.

‘

Structure d'anneaux

On dit que $(A, +, .)$ est un anneau si

- $(A, +)$ est un groupe commutatif ;
- . est une loi de composition interne associative et distributive par rapport à la loi $+$.

‘

- Si la loi . est commutative, on dit que l'anneau A est commutatif.

Structure d'anneaux

On dit que $(A, +, .)$ est un anneau si

- $(A, +)$ est un groupe commutatif ;
- . est une loi de composition interne associative et distributive par rapport à la loi $+$.

‘

- Si la loi . est commutative, on dit que l'anneau A est commutatif.
- Si la loi . admet un élément neutre(1_A ou 1), on dit que l'anneau A est unitaire.

Structure d'anneaux

On dit que $(A, +, .)$ est un anneau si

- $(A, +)$ est un groupe commutatif ;
- . est une loi de composition interne associative et distributive par rapport à la loi $+$.

‘

- Si la loi . est commutative, on dit que l'anneau A est commutatif.
- Si la loi . admet un élément neutre(1_A ou 1), on dit que l'anneau A est unitaire.
- Soit $B \subseteq A$. On dit que B est un sous anneau de A si $(B, +, .)$ est un anneau.

Structure d'anneaux

On dit que $(A, +, .)$ est un anneau si

- $(A, +)$ est un groupe commutatif ;
- . est une loi de composition interne associative et distributive par rapport à la loi $+$.

‘

- Si la loi . est commutative, on dit que l'anneau A est commutatif.
- Si la loi . admet un élément neutre(1_A ou 1), on dit que l'anneau A est unitaire.
- Soit $B \subseteq A$. On dit que B est un sous anneau de A si $(B, +, .)$ est un anneau.
- On appelle **caractéristique** de A l'ordre additif (s'il est fini) de 1_A ; si l'ordre additif de 1_A est infini on dit que A est de caractéristique nulle.

Dans la suite, nous ne considérerons que des anneaux commutatifs unitaires.

Idéaux

Soient $(A, +, .)$ un anneau et $I \subseteq A$

- . On dit que I est un idéal de A si $(I, +)$ est un groupe commutatif et $A.I \subseteq I$ (i.e. $\forall (a, b) \in A \times I, ax \in I$).

Idéaux

Soient $(A, +, .)$ un anneau et $I \subseteq A$

- . On dit que I est un idéal de A si $(I, +)$ est un groupe commutatif et $A.I \subseteq I$ (i.e. $\forall (a, b) \in A \times I, ax \in I$).
- On dit qu'un idéal I est **premier** si $I \neq A$ et $\forall a, b \in A$ on a : $ab \in I \Longrightarrow a \in I$ ou $b \in I$.
- On dit q'un idéal I est **maximal** si $I \neq A$ et si J est un idéal de A tel que $I \subset J$, alors $J = I$ ou $J = A$.

Idéaux

Soient $(A, +, .)$ un anneau et $I \subseteq A$

- . On dit que I est un idéal de A si $(I, +)$ est un groupe commutatif et $A.I \subseteq I$ (i.e. $\forall (a, b) \in A \times I, ax \in I$).
- On dit qu'un idéal I est **premier** si $I \neq A$ et $\forall a, b \in A$ on a : $ab \in I \Longrightarrow a \in I$ ou $b \in I$.
- On dit q'un idéal I est **maximal** si $I \neq A$ et si J est un idéal de A tel que $I \subset J$, alors $J = I$ ou $J = A$.
- Si I est un idéal de A, alors l'ensemble $A/I := \{a + I \ | a \in A\}$ munit de l' addition $\overline{+}$: $(a + I)\overline{+}(b + I) = (a + b) + I$ et de la multiplication $(a + I)(b + I) = ab + I$ est un anneau appelé anneau quotient de A par I.

Idéaux

Soient $(A, +, .)$ un anneau et $I \subseteq A$

- . On dit que I est un idéal de A si $(I, +)$ est un groupe commutatif et $A.I \subseteq I$ (i.e. $\forall (a, b) \in A \times I, ax \in I$).
- On dit qu'un idéal I est **premier** si $I \neq A$ et $\forall a, b \in A$ on a : $ab \in I \Longrightarrow a \in I$ ou $b \in I$.
- On dit q'un idéal I est **maximal** si $I \neq A$ et si J est un idéal de A tel que $I \subset J$, alors $J = I$ ou $J = A$.
- Si I est un idéal de A, alors l'ensemble $A/I := \{a + I \ | a \in A\}$ munit de l' addition $\overline{+}$: $(a + I)\overline{+}(b + I) = (a + b) + I$ et de la multiplication $(a + I)(b + I) = ab + I$ est un anneau appelé anneau quotient de A par I.

Élements particuliers

- Un élément **non nul** $a \in A$ est appelé **diviseur de zéro** si $\exists b(\neq 0) \in A$ tel que $ab = 0$.
  Si A ne contient aucun diviseur de zero, on dit que A est **intègre**.

Élements particuliers

- Un élément **non nul** $a \in A$ est appelé **diviseur de zéro** si $\exists b(\neq 0) \in A$ tel que $ab = 0$.
  Si A ne contient aucun diviseur de zero, on dit que A est **intègre**.
- Un élément $a \in A$ est dit **inversible** si $\exists b \in A / ab = 1$.
  Si tous les éléments non nuls de A sont inversibles, on dit que A est un **corps**.

Élements particuliers

- Un élément **non nul** $a \in A$ est appelé **diviseur de zéro** si $\exists b(\neq 0) \in A$ tel que $ab = 0$.
  Si A ne contient aucun diviseur de zero, on dit que A est **intègre**.
- Un élément $a \in A$ est dit **inversible** si $\exists b \in A / ab = 1$.
  Si tous les éléments non nuls de A sont inversibles, on dit que A est un **corps**. Autrement dit un anneau $(A, +, .)$ est un corps si et seulement si $(A \setminus \{0\}, .)$ est un groupe.
- On dit qu'un corps L est une extension d'un corps $\mathbb{K}$ si $\mathbb{K}$ est un sous corps de L. On note $L/\mathbb{K}$.

Élements particuliers

- Un élément **non nul** $a \in A$ est appelé **diviseur de zéro** si $\exists b(\neq 0) \in A$ tel que $ab = 0$.
  Si A ne contient aucun diviseur de zero, on dit que A est **intègre**.
- Un élément $a \in A$ est dit **inversible** si $\exists b \in A / ab = 1$.
  Si tous les éléments non nuls de A sont inversibles, on dit que A est un **corps**. Autrement dit un anneau $(A, +, .)$ est un corps si et seulement si $(A \setminus \{0\}, .)$ est un groupe.
- On dit qu'un corps L est une extension d'un corps $\mathbb{K}$ si $\mathbb{K}$ est un sous corps de L. On note $L/\mathbb{K}$.

Proposition

La caractéristique d'un corps est soit un nombre premier soit égale à 0.

▷ Soit $\mathbb{K}$ un corps de caractéristique n. Supposons que n n'est pas premier ; $n = pq$. Alors $(pq)1_{\mathbb{K}} = (p1_{\mathbb{K}})(q1_{\mathbb{K}}) = 0 \Rightarrow p1_{\mathbb{K}} = 0$ ou $q1_{\mathbb{K}} = 0$.
Absurde. Alors n est premier.

Idéaux

Proposition

Soit A un anneau.

- Un idéal I de A est premier si et seulement si A/I est intègre.
- Un idéal I de A est maximal si et seulement si A/I est un corps.

Soit $S \subset A$, l'ensemble $< S >= \{\sum_{\text{finie}} a_i s_i / a_i \in A \text{ et } s_i \in S\}$ est un idéal de A appelé **idéal engendré** par S.

Idéaux

Proposition

Soit A un anneau.

- Un idéal I de A est premier si et seulement si A/I est intègre.
- Un idéal I de A est maximal si et seulement si A/I est un corps.

Soit $S \subset A$, l'ensemble $< S >= \{\sum_{\text{finie}} a_i s_i / a_i \in A \text{ et } s_i \in S\}$ est un idéal de A appelé **idéal engendré** par S.
Si $S = \{s\}$, on dit que l'idéal $< s >:= sA = \{sa \ : \ a \in A\}$ est **principal**.

Anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $\mathbb{Z}$ l'anneau des entiers relatifs.

- Idéaux de $\mathbb{Z}$: $n\mathbb{Z}$.
- Idéaux premiers et maximaux de $\mathbb{Z}$: $p\mathbb{Z}$, où p est un nombre premier.
- L'anneau des entiers modulo p, $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z} = \{0, 1, \cdots, p-1\}$ est un corps fini à p éléments.

Exemple : $\mathbb{Z}_4$ n'est pas un corps car 4 n'est pas premier. Existe-il un corps de 4 éléments ?

$\mathbb{F}_4$

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

et

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

où $\alpha^2+\alpha+1=0$.

Anneaux de polynômes dans un corps

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ l' anneau des polynômes à coefficients dans $\mathbb{K}$.

- $\mathbb{K}[X]$ est euclidien i.e. $\mathbb{K}[X]$ est intègre et $\forall f \in \mathbb{K}[X],\ g \in \mathbb{K}[X] \setminus \{0\},\ \exists\ Q, R \in \mathbb{K}[X]$ tel que $f = gQ + R$ avec $\deg(R) < \deg(g)$.

Anneaux de polynômes dans un corps

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ l' anneau des polynômes à coefficients dans $\mathbb{K}$.

- $\mathbb{K}[X]$ est euclidien i.e. $\mathbb{K}[X]$ est intègre et $\forall f \in \mathbb{K}[X],\ g \in \mathbb{K}[X] \setminus \{0\},\ \exists\ Q, R \in \mathbb{K}[X]$ tel que $f = gQ + R$ avec $\deg(R) < \deg(g)$.
- $\mathbb{K}[X]$ est principal i.e. tout idéal non nul de $\mathbb{K}[X]$ est engendré par un élément.

Anneaux de polynômes dans un corps

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ l' anneau des polynômes à coefficients dans $\mathbb{K}$.

- $\mathbb{K}[X]$ est euclidien i.e. $\mathbb{K}[X]$ est intègre et $\forall f \in \mathbb{K}[X],\ g \in \mathbb{K}[X] \setminus \{0\},\ \exists\ Q, R \in \mathbb{K}[X]$ tel que $f = gQ + R$ avec $\deg(R) < \deg(g)$.
- $\mathbb{K}[X]$ est principal i.e. tout idéal non nul de $\mathbb{K}[X]$ est engendré par un élément.
- On dit qu'un polynôme de degré strictement positif f est irréductible sur $\mathbb{K}$ si ses seuls diviseurs sont les polynômes constants et les polynômes qui lui sont associés (i.e. c'est-à-dire les polynômes de la forme $\lambda\ f$).

Anneaux de polynômes dans un corps

Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ l' anneau des polynômes à coefficients dans $\mathbb{K}$.

- $\mathbb{K}[X]$ est euclidien i.e. $\mathbb{K}[X]$ est intègre et $\forall f \in \mathbb{K}[X],\ g \in \mathbb{K}[X] \setminus \{0\},\ \exists\ Q, R \in \mathbb{K}[X]$ tel que $f = gQ + R$ avec $\deg(R) < \deg(g)$.
- $\mathbb{K}[X]$ est principal i.e. tout idéal non nul de $\mathbb{K}[X]$ est engendré par un élément.
- On dit qu'un polynôme de degré strictement positif f est irréductible sur $\mathbb{K}$ si ses seuls diviseurs sont les polynômes constants et les polynômes qui lui sont associés (i.e. c'est-à-dire les polynômes de la forme $\lambda\ f$).
- Tout polynôme f de $\mathbb{K}[X]$ se décompose en produit de facteurs irréductibles et cette décomposition est unique à permutation près des facteurs et des constantes non nuls.

Anneaux de polynômes dans un corps

Soient $\mathbb{K}$ un corps et f un polynôme de degré n dans $\mathbb{K}[X]$.

- $\mathbb{K}[X]/ < f >$ est un $\mathbb{K}$-espace vectoriel de dimension n.
- Une base est donnée par $(1, \alpha, \cdots, \alpha^{n-1})$ où $\alpha := X + < f >$.

Anneaux de polynômes dans un corps

Soient $\mathbb{K}$ un corps et f un polynôme de degré n dans $\mathbb{K}[X]$.

- $\mathbb{K}[X]/ < f >$ est un $\mathbb{K}$-espace vectoriel de dimension n.
- Une base est donnée par $(1, \alpha, \cdots, \alpha^{n-1})$ où $\alpha := X + < f >$.

Proposition

Tout idéal maximal de $\mathbb{K}[X]$ est engendré par un polynôme irréductible.

Preuve Soient f un polynôme irréductible de $\mathbb{K}[X]$ et $\overline{g(x)} \in \mathbb{K}[X]/ < f(x) >$ avec $\overline{g(x)} \neq \overline{0}$. Alors $f(x) \nmid g(x)$ et $\text{pgcd}(f(x), g(x)) = 1$. D' après le lemme de Bezout, il existe des polynômes $h(x), k(x) \in \mathbb{K}[X]$ tel que $h(x)f(x) + k(x)g(x) = 1$. Alors $\overline{k(x)g(x)} = \overline{1}$. Donc $\mathbb{K}[X]/ < f(x) >$ est un corps. □

Groupe multiplicatif

L'ensemble $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$, i.e. l'ensemble des éléments inversibles de $\mathbb{Z}_p$ est un groupe cyclique.

Exemple : Vérifier si $2, 3, 5$ sont des générateurs du groupe multiplicatif $\mathbb{Z}_7^*$.

Groupe multiplicatif

L'ensemble $\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$, i.e. l'ensemble des éléments inversibles de $\mathbb{Z}_p$ est un groupe cyclique.
Exemple : Vérifier si $2, 3, 5$ sont des générateurs du groupe multiplicatif $\mathbb{Z}_7^*$.

Proposition

Soit $\mathbb{K}$ un corps fini à q éléments. Le groupe multiplicatif $\mathbb{K}^*$ est cyclique.

Preuve Soit e l'exposant du groupe $\mathbb{K}^*$ i.e. le ppcm des ordres de tous les éléments de $\mathbb{K}^*$. IL existe un élément $a \in \mathbb{K}^*$ d'ordre e.
$\forall x \in \mathbb{K}^*;\ x^{q-1} = 1$, alors $e \leq q-1$. De plus $\forall x \in \mathbb{K}^*;\ x^e = 1$ et le polynôme $X^e - 1$ admet au plus e racines, donc $q - 1 \leq e$; d'où $q - 1 = e$. $\square$.

Polynôme primitif

Soit $\mathbb{K}$ un corps fini à q éléments.

1. On appelle **élément primitif** d'un corps fini $\mathbb{K}$ tout générateur de $\mathbb{K}^*$. Un polynôme unitaire irreductible de $\mathbb{K}[X]$ qui a pour racine un élément primitif de $\mathbb{K}$ est appelé **polynôme primitif**

Polynôme primitif

Soit $\mathbb{K}$ un corps fini à q éléments.

1. On appelle **élément primitif** d'un corps fini $\mathbb{K}$ tout générateur de $\mathbb{K}^*$. Un polynôme unitaire irreductible de $\mathbb{K}[X]$ qui a pour racine un élément primitif de $\mathbb{K}$ est appelé **polynôme primitif**
2. Si $\mathbb{K}^* =< \alpha >$, alors α^k est aussi un élément primitif de $\mathbb{K}$ si et seulement si $pgcd(k, q-1) = 1$.

Polynôme primitif

Soit $\mathbb{K}$ un corps fini à q éléments.

1. On appelle **élément primitif** d'un corps fini $\mathbb{K}$ tout générateur de $\mathbb{K}^*$. Un polynôme unitaire irreductible de $\mathbb{K}[X]$ qui a pour racine un élément primitif de $\mathbb{K}$ est appelé **polynôme primitif**
2. Si $\mathbb{K}^* =< \alpha >$, alors α^k est aussi un élément primitif de $\mathbb{K}$ si et seulement si $pgcd(k, q-1) = 1$.
   Ainsi le nombre d' éléments primitifs de $\mathbb{K}$ est égal au cardinal de la fonction indicatrice d' Euler :

$$\phi(q-1) := \{k \in \{1; 2; \cdots; q-2\} \mid \text{pgcd}(k, q-1) = 1\}.$$

Polynôme primitif

Soit $\mathbb{K}$ un corps fini à q éléments.

1. On appelle **élément primitif** d'un corps fini $\mathbb{K}$ tout générateur de $\mathbb{K}^*$.
   Un polynôme unitaire irreductible de $\mathbb{K}[X]$ qui a pour racine un élément primitif de $\mathbb{K}$ est appelé **polynôme primitif**
2. Si $\mathbb{K}^* =< \alpha >$, alors α^k est aussi un élément primitif de $\mathbb{K}$ si et seulement si $pgcd(k, q-1) = 1$.
   Ainsi le nombre d' éléments primitifs de $\mathbb{K}$ est égal au cardinal de la fonction indicatrice d' Euler :

$$\phi(q-1) := \{k \in \{1; 2; \cdots; q-2\} \mid \text{pgcd}(k, q-1) = 1\}.$$

3. Toutes les racines d'un polynôme primitif sont aussi des éléments primitifs.

Polynôme primitif

Soit $\mathbb{K}$ un corps fini à q éléments.

1. On appelle **élément primitif** d'un corps fini $\mathbb{K}$ tout générateur de $\mathbb{K}^*$. Un polynôme unitaire irreductible de $\mathbb{K}[X]$ qui a pour racine un élément primitif de $\mathbb{K}$ est appelé **polynôme primitif**
2. Si $\mathbb{K}^* =< \alpha >$, alors α^k est aussi un élément primitif de $\mathbb{K}$ si et seulement si $pgcd(k, q-1) = 1$.
   Ainsi le nombre d' éléments primitifs de $\mathbb{K}$ est égal au cardinal de la fonction indicatrice d' Euler :

$$\phi(q-1) := \{k \in \{1; 2; \cdots; q-2\} \mid \text{pgcd}(k, q-1) = 1\}.$$

3. Toutes les racines d'un polynôme primitif sont aussi des éléments primitifs.
4. On dit que $\xi \in \mathbb{K}$ est une racine primitive n-ième de l'unité si son ordre multiplicatif est égale à n.
5. $\mathbb{K}$ contient une racine primitive n-ième de l'unité si et seulement si $n \mid (q-1)$

Element primitif

Pour trouver un élément primitif d'un corps fini à $\mathbb{F}_q$ éléments, on peut procéder comme suit :

1. choisir un élément arbitraire $\alpha_1 \in \mathbb{F}_q^*$
2. si α_1 n'est pas un élément primitif, choisir un autre élément $\alpha_2 \in \mathbb{F}_q^* \setminus < \alpha_1 >$
3. si α_2 n'est pas également un élément primitif, trouver des entiers d_1, d_2 tels que $d_1 \mid ord(\alpha_1)$ et $d_2 \mid ord(\alpha_2)$, avec $pgcd(d_1, d_2) = 1$.
4. Considerer $\alpha_3 = \alpha_1^{ord(\alpha_1)/d_1} \alpha_2^{ord(\alpha_2)/d_2}$. Ainsi $ord(\alpha_3) = d_1 d_2 = ppcm(ord(\alpha_1), ord(\alpha_2))$.
5. Continuer le processus et trouver $\alpha_k \in \mathbb{F}_q$ tel que $ord(\alpha_k) = q - 1$.

Exercice : Trouver un élément primitif de $\mathbb{Z}_{41}$.

Ordre d'un corps fini

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

- $\mathbb{Z}_p$ est un sous corps de $\mathbb{K}$. C'est le plus petit sous corps contenu dans $\mathbb{K}$. On dit dans ce cas que $\mathbb{K}$ est le sous corps premier de $\mathbb{K}$.

Ordre d'un corps fini

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

- $\mathbb{Z}_p$ est un sous corps de $\mathbb{K}$. C'est le plus petit sous corps contenu dans $\mathbb{K}$. On dit dans ce cas que $\mathbb{K}$ est le sous corps premier de $\mathbb{K}$.
- $|\mathbb{K}| = p^n$, où n est un entier naturel non nul.
  ▷ $\mathbb{Z}_p \subset \mathbb{K}$ et $\mathbb{K}$ est un $\mathbb{Z}_p$-espace vectoriel de dimension fini(noté n).

Ordre d'un corps fini

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

- $\mathbb{Z}_p$ est un sous corps de $\mathbb{K}$. C'est le plus petit sous corps contenu dans $\mathbb{K}$. On dit dans ce cas que $\mathbb{K}$ est le sous corps premier de $\mathbb{K}$.
- $|\mathbb{K}| = p^n$, où n est un entier naturel non nul.
  ▷ $\mathbb{Z}_p \subset \mathbb{K}$ et $\mathbb{K}$ est un $\mathbb{Z}_p$-espace vectoriel de dimension fini(noté n).
- $(a+b)^{p^n} = a^{p^n} + b^{p^n}$, $\forall a, b \in \mathbb{K}$.
  Dans la suite $\mathbb{F}_q$ désignera un corps fini à q éléments(q puissance d'un nombre premier)

Construction corps finis

Soit $\mathbb{F}_q$ un corps fini à q éléments.

1. $\forall \alpha \in \mathbb{F}_q$, on a $\alpha^q = \alpha$, alors $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ i.e. $\mathbb{F}_q$ est une extension de $\mathbb{F}_p$ dans laquelle $X^q - X (\in \mathbb{F}_p[X])$ est scindée en racines simples.

Construction corps finis

Soit $\mathbb{F}_q$ un corps fini à q éléments.

1. $\forall \alpha \in \mathbb{F}_q$, on a $\alpha^q = \alpha$, alors $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ i.e. $\mathbb{F}_q$ est une extension de $\mathbb{F}_p$ dans laquelle $X^q - X (\in \mathbb{F}_p[X])$ est scindée en racines simples.
2. Si f un polynôme irréductible de degré n sur $\mathbb{F}_q$, alors $\mathbb{F}_q[X]/ < f(X) > (\cong F_q[\alpha])$ est un corps fini à q^n éléments, où $\alpha = X + < f(X) >$.
   $\mathbb{F}_{q^n}$ est le corps de décomposition du polynôme $X^{q^n} - X$ sur $\mathbb{F}_q$.

Construction corps finis

Soit $\mathbb{F}_q$ un corps fini à q éléments.

1. $\forall \alpha \in \mathbb{F}_q$, on a $\alpha^q = \alpha$, alors $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ i.e. $\mathbb{F}_q$ est une extension de $\mathbb{F}_p$ dans laquelle $X^q - X (\in \mathbb{F}_p[X])$ est scindée en racines simples.
2. Si f un polynôme irréductible de degré n sur $\mathbb{F}_q$, alors $\mathbb{F}_q[X]/ < f(X) > (\cong F_q[\alpha])$ est un corps fini à q^n éléments, où $\alpha = X + < f(X) >$.
   $\mathbb{F}_{q^n}$ est le corps de décomposition du polynôme $X^{q^n} - X$ sur $\mathbb{F}_q$.

La construction de corps finis est intrinsèquement liée à l'existence de polynômes irréductibles.

Théorème

Pour tout entier naturel n, il existe un polynôme unitaire irreductible de degré n dans $F_q[X]$.

Propriétés

Soient $\mathbb{F}_q$ un corps fini à q éléments et L une extension de $\mathbb{F}_q$. Soient $\alpha \in L$ et $f \in L[X]$. Alors

- $\alpha \in \mathbb{F}_q \Leftrightarrow \alpha^q = \alpha$
- $f \in \mathbb{F}_q[X] \Leftrightarrow f(X^q) = f(X)^q$.

Propriétés

Soient $\mathbb{F}_q$ un corps fini à q éléments et L une extension de $\mathbb{F}_q$. Soient $\alpha \in L$ et $f \in L[X]$. Alors

- $\alpha \in \mathbb{F}_q \Leftrightarrow \alpha^q = \alpha$
- $f \in \mathbb{F}_q[X] \Leftrightarrow f(X^q) = f(X)^q$.

Soient f est un polynome unitaire irréductible de degré n dans $\mathbb{F}_q[X]$, et $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/ < f >$.
Si $f(\alpha) = 0$ alors $f(\alpha^q) = 0$, et par itération, on deduit que les racines de f dans $\mathbb{F}_{q^n}$ sont $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$. Ils sont deux a deux distincts.

Tout élément $\beta \in \mathbb{F}_{q^n}$ est racine du polynôme $X^{q^n} - X$. En particulier $\alpha^{q^n} - \alpha = 0$ i.e. $X^{q^n} - X \equiv 0 \mod < f(x) >$. D'où $f \mid X^{q^n} - X$ dans $\mathbb{F}_q[X]$.

Tout élément $\beta \in \mathbb{F}_{q^n}$ est racine du polynôme $X^{q^n} - X$. En particulier $\alpha^{q^n} - \alpha = 0$ i.e. $X^{q^n} - X \equiv 0 \mod < f(x) >$. D'où $f \mid X^{q^n} - X$ dans $\mathbb{F}_q[X]$.

Proposition

Soit f un polynôme irréductible de degré d sur $\mathbb{F}_q[X]$. Alors $f(X) \mid \left(X^{q^n} - X\right)$ if and only if $d \mid n$.

Preuve Soient $\mathbb{F}_{q^d}[x] = \mathbb{F}_q[x]/ < f >$ et $\alpha := X + < f >$.
On suppose $f(X) \mid \left(X^{q^n} - X\right)$. Comme $f(\alpha) = 0$ alors $\alpha^{q^n} = \alpha$. Par division euclidienne, il existe t, r tels que $n = dt + r$ avec $0 \leq r < d$. On a $\alpha^{q^{dt+r}} = (\alpha^{q^{dt}})^{q^r} = \alpha^{q^r} = \alpha$ absurde car q^d est l' ordre de F_{q^d}. Donc $r = 0$.

Tout élément $\beta \in \mathbb{F}_{q^n}$ est racine du polynôme $X^{q^n} - X$. En particulier $\alpha^{q^n} - \alpha = 0$ i.e. $X^{q^n} - X \equiv 0 \mod < f(x) >$. D'où $f \mid X^{q^n} - X$ dans $\mathbb{F}_q[X]$.

Proposition

Soit f un polynôme irréductible de degré d sur $\mathbb{F}_q[X]$. Alors $f(X) \mid \left(X^{q^n} - X\right)$ if and only if $d \mid n$.

Preuve Soient $\mathbb{F}_{q^d}[x] = \mathbb{F}_q[x]/ < f >$ et $\alpha := X + < f >$.
On suppose $f(X) \mid \left(X^{q^n} - X\right)$. Comme $f(\alpha) = 0$ alors $\alpha^{q^n} = \alpha$. Par division euclidienne, il existe t, r tels que $n = dt + r$ avec $0 \leq r < d$. On a $\alpha^{q^{dt+r}} = (\alpha^{q^{dt}})^{q^r} = \alpha^{q^r} = \alpha$ absurde car q^d est l' ordre de F_{q^d}. Donc $r = 0$.
Réciproquement on suppose $d \mid n$. Puisque $\alpha^{q^d} = \alpha$ alors $\alpha^{q^n} = \alpha$ i.e. α est racine de $X^{q^n} - X$. De plus les éléments $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{d-1}}$ sont des racines deux à deux distinctes de $X^{q^n} - X$. Par conséquent f divise $X^{q^n} - X$. □

Tout élément $\beta \in \mathbb{F}_{q^n}$ est racine du polynôme $X^{q^n} - X$. En particulier $\alpha^{q^n} - \alpha = 0$ i.e. $X^{q^n} - X \equiv 0 \mod < f(x) >$. D'où $f \mid X^{q^n} - X$ dans $\mathbb{F}_q[X]$.

Proposition

Soit f un polynôme irréductible de degré d sur $\mathbb{F}_q[X]$. Alors $f(X) \mid \left(X^{q^n} - X\right)$ if and only if $d \mid n$.

Preuve Soient $\mathbb{F}_{q^d}[x] = \mathbb{F}_q[x]/ < f >$ et $\alpha := X + < f >$.
On suppose $f(X) \mid \left(X^{q^n} - X\right)$. Comme $f(\alpha) = 0$ alors $\alpha^{q^n} = \alpha$. Par division euclidienne, il existe t, r tels que $n = dt + r$ avec $0 \leq r < d$. On a $\alpha^{q^{dt+r}} = (\alpha^{q^{dt}})^{q^r} = \alpha^{q^r} = \alpha$ absurde car q^d est l' ordre de F_{q^d}. Donc $r = 0$.
Réciproquement on suppose $d \mid n$. Puisque $\alpha^{q^d} = \alpha$ alors $\alpha^{q^n} = \alpha$ i.e. α est racine de $X^{q^n} - X$. De plus les éléments $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{d-1}}$ sont des racines deux à deux distinctes de $X^{q^n} - X$. Par conséquent f divise $X^{q^n} - X$. □

▷ $F_{q^m} \subseteq F_{q^n} \Leftrightarrow m \mid n$

Unicité

Proposition

Deux corps finis ayant le même nombre d'éléments sont isomorphes.

Preuve Soient K et L des corps finis à p^n éléments. Il existe un polynôme irréductible $f \in \mathbb{F}_p[X]$, de degré n, tel que $K \cong \mathbb{F}_p[X]/ < f >$, $f \mid X^{p^n} - X \in \mathbb{F}_p[X]$. De plus L est aussi le corps de décomposition de $X^{p^n} - X$. Alors f possède une racine $\alpha \in L$. L'application

$$\begin{array}{rccc} \varphi : & \mathbb{F}_p[X] & \to & L \\ & g & \mapsto & g(\alpha) \end{array}$$

un morphisme d'anneaux surjectif et $\ker \varphi =< f >$. Alors $\mathbb{F}_p[X]/(f) \cong L$. □

Logarithme discret

On peut représenter les éléments de $\mathbb{F}_q$ sous deux formes : une représentation polynomiale et une représentation multiplicative où les éléments sont les puissances d'une racine primitive.

Logarithme discret

On peut représenter les éléments de $\mathbb{F}_q$ sous deux formes : une représentation polynomiale et une représentation multiplicative où les éléments sont les puissances d'une racine primitive.
Exemple : $\mathbb{F}_8 = \mathbb{F}_2[X]/ < X^3 + X + 1 >$; $\alpha = X + < X^3 + X + 1 >$.

Multiplicative	0	1	α	α^2	α^3	α^4	α^5	α^6
Polynomial	0	1	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$

Logarithme discret

On peut représenter les éléments de $\mathbb{F}_q$ sous deux formes : une représentation polynomiale et une représentation multiplicative où les éléments sont les puissances d'une racine primitive.
Exemple : $\mathbb{F}_8 = \mathbb{F}_2[X]/ < X^3 + X + 1 >$; $\alpha = X + < X^3 + X + 1 >$.

Multiplicative	0	1	α	α^2	α^3	α^4	α^5	α^6
Polynomial	0	1	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$

Soit α un élément primitif de $\mathbb{F}_q$ et $\beta \in \mathbb{F}_q$. Le problème du logarithme discret consiste à trouver l' entier i tel que l'on ait $\beta = \alpha^i$, $0 \leq i \leq q - 2$. L'entier i noté $log_\alpha(\beta)$ est appelé logarithme discret de base α de β.

Automorphisme de Frobenius

Soit $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension de corps finis de caractéristique p. L'application

$$\begin{aligned} Frob_{q^n} : \quad & \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n} \\ & a \longmapsto a^q \end{aligned}$$

est un automorphisme de $\mathbb{F}_{q^n}$ qui laisse invariant les éléments de $\mathbb{F}_q$.
$Frob_{q^n}$ est appelé $\mathbb{F}_q$- automorphisme de Frobenius de $\mathbb{F}_{q^n}$.

Automorphisme de Frobenius

Soit $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension de corps finis de caractéristique p. L'application

$$\begin{aligned} Frob_{q^n} : \quad & \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n} \\ & a \longmapsto a^q \end{aligned}$$

est un automorphisme de $\mathbb{F}_{q^n}$ qui laisse invariant les éléments de $\mathbb{F}_q$.
$Frob_{q^n}$ est appelé $\mathbb{F}_q$- automorphisme de Frobenius de $\mathbb{F}_{q^n}$.

1. $Frob_{q^n}^n = 1$ et $\{1, Frob_{q^n}, \cdots, Frob_{q^n}^{n-1}\}$ est un groupe cyclique (pour la loi de composition des applications), c'est le groupe de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_q$.

Automorphisme de Frobenius

Soit $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension de corps finis de caractéristique p. L'application

$$\begin{aligned} Frob_{q^n} : \quad & \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n} \\ & a \longmapsto a^q \end{aligned}$$

est un automorphisme de $\mathbb{F}_{q^n}$ qui laisse invariant les éléments de $\mathbb{F}_q$.
$Frob_{q^n}$ est appelé $\mathbb{F}_q$- automorphisme de Frobenius de $\mathbb{F}_{q^n}$.

1. $Frob_{q^n}^n = 1$ et $\{1, Frob_{q^n}, \cdots, Frob_{q^n}^{n-1}\}$ est un groupe cyclique (pour la loi de composition des applications), c'est le groupe de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_q$.
2. Si $d \mid n$, alors $Frob_{q^n}^d$ est l' automorphisme de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_{q^d}$ et représente le générateur du groupe de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_{q^d}$ (c'est un groupe d'ordre n/d).

Automorphisme de Frobenius

Soit $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension de corps finis de caractéristique p. L'application

$$\begin{aligned} Frob_{q^n} : \quad & \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n} \\ & a \longmapsto a^q \end{aligned}$$

est un automorphisme de $\mathbb{F}_{q^n}$ qui laisse invariant les éléments de $\mathbb{F}_q$.
$Frob_{q^n}$ est appelé $\mathbb{F}_q$- automorphisme de Frobenius de $\mathbb{F}_{q^n}$.

1. $Frob_{q^n}^n = 1$ et $\{1, Frob_{q^n}, \cdots, Frob_{q^n}^{n-1}\}$ est un groupe cyclique (pour la loi de composition des applications), c'est le groupe de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_q$.
2. Si $d \mid n$, alors $Frob_{q^n}^d$ est l' automorphisme de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_{q^d}$ et représente le générateur du groupe de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_{q^d}$ (c'est un groupe d'ordre n/d).
3. On pose $\sigma := Frob_{q^n}$ et $\alpha \in \mathbb{F}_{q^n}$. Le polynôme unitaire de plus petit degré sur $\mathbb{F}_q$ dont α est racine est appelé polynôme minimal de α sur $\mathbb{F}_q$ (Il est irréductible sur $\mathbb{F}_q$) .
   Il est défini par $m(X) := (X - \alpha)(X - \sigma(\alpha)) \cdots (X - \sigma(\alpha)^{d-1})$, où d est le plus petit entier tel que $\sigma^d(\alpha) = \alpha$. (Noter que $d \mid n$)

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

Si $N = np^k$, avec $pgcd(n, p) = 1$ alors $X^N - 1 = (X^n - 1)^{p^k}$. Il suffit donc de considérer la factorisation $X^n - 1$ avec $pgcd(n, p) = 1$. Dans ce cas $X^n - 1$ se décompose en facteurs simples.
Soit $\mathbb{F}_{q^m}$ le corps de décomposition de $X^n - 1$ sur $\mathbb{F}_q$. Soit α un élément primitif de $\mathbb{F}_{q^m}$ et $\xi = \alpha^{(q^m-1)/n}$ est une racine primitive n-ième de l'unité. Alors $1, \xi, \xi^2, \cdots, \xi^{n-1}$ sont les racines de $X^n - 1$. Soit m_{ξ^i} le polynôme minimal associé à ξ^i, on a
$m_{\xi^i}(X) = (X - \xi^i)(X - \sigma(\xi^i)) \cdots (X - \sigma(\xi^i)^{m_i-1}) =$
$(X - \xi^i)(X - \xi^{iq}) \cdots (X - \xi^{iq^{m_i-1}})$, où m_i est le plus petit entier tel que $\sigma^{m_i}(\xi^i) = \xi^i$.

Classe cyclotomique

On appelle q-classe cyclotomique modulo n contenant i l'ensemble défini par

$$C_q(i,n) = \{i, iq, iq^2, ..., iq^{m_i-1}\}$$

où m_i est le plus petit entier naturel vérifiant $iq^{m_i} \equiv i \mod n$. Soit I un ensemble des représentants de chaque classe, la décomposition de $X^n - 1$ en produit de facteurs unitaires irréductibles est donnée par :
$X^n - 1 = \prod_{i \in I} m_{\xi^i}(X)$ où $m_{\xi^i}(X) = \prod_{j \in C_q(i,n)} (X - \xi^j)$, et ξ est une racine primitive n-ième de l'unité.

Factoriser sur $\mathbb{F}_2$ le polynôme $X^7 - 1$ en produit de facteurs irréductibles.

Factoriser sur $\mathbb{F}_2$ le polynôme $X^7 - 1$ en produit de facteurs irréductibles.

- $C_2(0,7) = \{0\},\ C_2(1,7) = \{1,2,4\},\ C_2(3,7) = \{3,6,5\}$.

Factoriser sur $\mathbb{F}_2$ le polynôme $X^7 - 1$ en produit de facteurs irréductibles.

- $C_2(0,7) = \{0\},\ C_2(1,7) = \{1,2,4\},\ C_2(3,7) = \{3,6,5\}$.
- Un élément primitif de $\mathbb{F}_8 = \mathbb{F}_2[X]/ < X^3 + X + 1 >$ est une racine primitive 7-ième de l'unité.

Factoriser sur $\mathbb{F}_2$ le polynôme $X^7 - 1$ en produit de facteurs irréductibles.

- $C_2(0,7) = \{0\},\ C_2(1,7) = \{1,2,4\},\ C_2(3,7) = \{3,6,5\}$.
- Un élément primitif de $\mathbb{F}_8 = \mathbb{F}_2[X]/ < X^3 + X + 1 >$ est une racine primitive 7-ième de l'unité.
- $m_{\alpha^0}(X) = (X + 1)$
- $m_{\alpha^1}(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^4) = X^3 + X + 1$
- $m_{\alpha^3}(X) = (X - \alpha^3)(X - \alpha^5)(X - \alpha^6) = X^3 + X^2 + 1$.

Factoriser sur $\mathbb{F}_2$ le polynôme $X^7 - 1$ en produit de facteurs irréductibles.

- $C_2(0,7) = \{0\},\ C_2(1,7) = \{1,2,4\},\ C_2(3,7) = \{3,6,5\}$.
- Un élément primitif de $\mathbb{F}_8 = \mathbb{F}_2[X]/ < X^3 + X + 1 >$ est une racine primitive 7-ième de l'unité.
- $m_{\alpha^0}(X) = (X + 1)$
- $m_{\alpha^1}(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^4) = X^3 + X + 1$
- $m_{\alpha^3}(X) = (X - \alpha^3)(X - \alpha^5)(X - \alpha^6) = X^3 + X^2 + 1$.
- $X^7 - 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$.

Utiliser sans modération les logiciels de calcul formel tel que **SageMath**.


MacWilliams, F.J. AND Sloane, N.J.A. *The Theory of Error-Correcting Codes*, Bell Laboratories Murray Hill NJ 07974 U.S.A, 1981.


Wan, Zhe-Xian *Lectures on finite fields and Galois Rings*, World Scientific , 2003.


Bini, G. AND Flamini, F. *Finite Commutative Rings and Their Applications*, Springer, 2002.