Séance 2 : Structure des corps finis

Hervé Talé Kalachi

1 Théorie des corps finis

Définition 1.1 (Corps fini)**.** Un corps fini est un corps commutatif contenant un nombre fini d'éléments. L'ordre d'un corps fini est son nombre d'éléments.

Remarque 1.1 (Motivation historique)**.** Les corps finis furent étudiés initialement par Galois (1830) pour résoudre des problèmes de théorie des nombres. Leur importance moderne vient des applications en :

- Cryptographie (protocoles ECC, AES)
- Théorie des codes (codes correcteurs)
- Mathématiques discrètes

Théorème 1.1 (Caractérisation des corps finis)**.** Pour tout nombre premier p et pour tout entier $n \geq 1$ il existe un corps fini $\mathbb{F}$ tel que $|\mathbb{F}| = p^n$. De plus, deux corps finis de même ordre sont isomorphes.

Démonstration. **Existence :** Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Considérons :

$$K = \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$$

Alors K est un sous-corps de $\overline{\mathbb{F}_p}$ avec exactement p^n éléments.

Unicité : Soient K_1 et K_2 deux corps à p^n éléments. Alors :

- Ils contiennent tous deux $\mathbb{F}_p$ comme sous-corps premier
- Leurs groupes multiplicatifs K_1^* et K_2^* sont cycliques d'ordre $p^n - 1$
- Tout générateur α de K_1^* vérifie $\mathbb{F}_p(\alpha) = K_1$
- Le polynôme minimal de α sur $\mathbb{F}_p$ est irréductible de degré n

Ceci induit un isomorphisme $K_1 \cong \mathbb{F}_p[X]/(f) \cong K_2$.

Construction explicite : Pour $f \in \mathbb{F}_p[X]$ irréductible de degré n :

- $\mathbb{F}_p[X]/(f)$ est un anneau principal
- L'irréductibilité de f implique que c'est un corps
- La dimension comme $\mathbb{F}_p$-espace vectoriel est n, donc p^n éléments

□

2 Construction de $\mathbb{F}_4$

2.1 Étape 1 : Choix du polynôme

Prenons $f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$. Vérifions l'irréductibilité :

$$f(0) = 1 \neq 0$$
$$f(1) = 1 + 1 + 1 = 1 \neq 0 \quad (\text{car } 1 + 1 = 0 \text{ en } \mathbb{F}_2)$$

2.2 Étape 2 : Structure algébrique

Éléments : $0, 1, \alpha, \alpha + 1$ où $\alpha^2 = \alpha + 1$

Remarque 2.1 (Calcul des inverses)**.** Par algorithme d'Euclide étendu :

$$(1 + \alpha)^{-1} = \alpha$$
$$\alpha^{-1} = 1 + \alpha$$

2.3 Tables d'opérations

Table d'addition :

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

Table de multiplication :

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

3 Applications avancées

3.1 Algorithme d'Euclide étendu pour polynômes

Input: Polynômes $a(X), b(X)$ non nuls
Output: (g, u, v) tels que $g = pgcd(a, b) = au + bv$
$r_0 \leftarrow a,\ r_1 \leftarrow b;$
$s_0 \leftarrow 1,\ s_1 \leftarrow 0;$
$t_0 \leftarrow 0,\ t_1 \leftarrow 1;$
while $r_1 \neq 0$ **do**
  $q \leftarrow r_0 \div r_1;$
  $r_0, r_1 \leftarrow r_1, r_0 - qr_1;$
  $s_0, s_1 \leftarrow s_1, s_0 - qs_1;$
  $t_0, t_1 \leftarrow t_1, t_0 - qt_1;$
end
return (r_0, s_0, t_0);

Algorithm 1: Euclide étendu polynomial

3.2 Applications pratiques

- **Cryptographie :** Implémentation du Rijndael (AES) utilisant $\mathbb{F}_{2^8}$
- **Codes correcteurs :** Codes Reed-Solomon dans les QR codes
- **Arithmétique modulaire :** Optimisation des calculs dans les extensions de corps

Exemple 3.1 (AES MixColumns)**.** Opération utilisant la multiplication matricielle sur $\mathbb{F}_{2^8}$ avec polynôme irréductible $x^8 + x^4 + x^3 + x + 1$.

4 Exercices enrichis

4.1 Exercice 1 : Construction de $\mathbb{F}_8$

Construire $\mathbb{F}_8$ avec le polynôme $X^3 + X + 1 \in \mathbb{F}_2[X]$.

Indication. Éléments : $\{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$
Relation : $\alpha^3 = \alpha + 1$ □

4.2 Exercice 2 : Calcul d'inverse

Trouver l'inverse de $\alpha^2 + 1$ dans $\mathbb{F}_2[X]/(X^3 + X + 1)$.

Solution guidée. 1. Appliquer l'algorithme d'Euclide étendu à $f(X) = X^3 + X + 1$ et $g(X) = X^2 + 1$
2. Exprimer 1 comme combinaison linéaire
3. Lire l'inverse dans les coefficients □

4.3 Exercice 3 : Programmation

Implémenter l'addition dans $\mathbb{F}_{16}$ avec représentation polynomiale.

```
def add_f16(a, b, irred_poly=0x13):
    return a ^ b  # XOR bit a bit

# Test
assert add_f16(0xA, 0xB) == 0x1  # 1010 XOR 1011 = 0001
```

5 Compléments théoriques

5.1 Théorème de la base normale

Théorème 5.1 (Base normale)**.** Toute extension finie $\mathbb{F}_{p^n}/\mathbb{F}_p$ possède une base de la forme $\{\alpha, \alpha^p, \alpha^{p^2}, ..., \alpha^{p^{n-1}}\}$ pour un α bien choisi.

5.2 Polynômes irréductibles

Proposition 5.1 (Densité des irréductibles)**.** Le nombre de polynômes irréductibles unitaires de degré n sur $\mathbb{F}_p$ est :

$$\frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}$$

où μ est la fonction de Möbius.

Input: Polynôme $f \in \mathbb{F}_p[X]$, degré n
Output: Vrai si f est irréductible
for $k = 1$ *à* $\lfloor n/2 \rfloor$ **do**
    Calculer $pgcd(f, X^{p^k} - X)$;
    if $pgcd \neq 1$ **then**
        Retourner Faux
    end
end
Retourner Vrai;

Algorithm 2: Test d'irréductibilité de Rabin