Algèbre 17 – Corps finis. Applications.

1 Structure des corps finis

1.1 Caractéristique, cardinal

K: corps fini. Image de $\mathbb{Z}$ dans K: isomorphe à un $\mathbb{Z}/p\mathbb{Z}$ (p premier: *caractéristique*). Corps des fractions isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, *sous-corps premier* de K.

$\sigma : x \mapsto x^p$ est un automorphisme de K.

K: extension de $\mathbb{F}_p$ de degré n. On a $|K| = p^n$.

1.2 Existence et unicité des corps finis

Théorème 1 (existence) *Pour tout p premier et tout $n \geqslant 1$, il existe un corps fini à $q = p^n$ éléments: le corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$, noté $\mathbb{F}_q$.*

Théorème 2 (unicité) *Tout corps à q éléments est isomorphe à $\mathbb{F}_q$.*

1.3 Conditions suffisantes (cas fini)

Théorème 3 *Tout anneau intègre fini est un corps.*

Théorème 4 (Wedderburn) *Tout anneau à division fini est un corps.*

1.4 Sous-corps, clôture algébrique

Théorème 5 *Soit $\mathbb{F}_q$ un corps fini à $q = p^n$ éléments. Alors tout sous-corps de $\mathbb{F}_q$ est d'ordre p^m où $m \mid n$. Réciproquement, si $m \mid n$, $\mathbb{F}_q$ a un unique sous-corps $\mathbb{F}_r$ d'ordre $r = p^m$.*

$\mathbb{F}_r = \{x \in \mathbb{F}_q : x^r - x = 0\}$

On peut alors définir: $\widehat{\mathbb{F}_p} = \bigcup_{n \geqslant 1} \mathbb{F}_{p^{n!}}$. C'est la clôture algébrique de tout $\mathbb{F}_q$ avec $q = p^n$.

2 Groupe multiplicatif de $\mathbb{F}_q$

Théorème 6 *Le groupe multiplicatif $\mathbb{F}_q^*$ du corps fini $\mathbb{F}_q$ est cyclique d'ordre $q - 1$.*

Application: logarithme discret, cryptographie.

Théorème 7 *Si $p = 2$, tout élément de $\mathbb{F}_q$ est un carré. Si $p \neq 2$, les carrés de $\mathbb{F}_q^*$ forment un sous-groupe d'indice 2 de $\mathbb{F}_q^*$, noyau de l'homomorphisme $\eta : x \mapsto x^{(q-1)/2}$, à valeurs dans $\{\pm 1\}$.*

η est appelé *caractère quadratique* de $\mathbb{F}_q$.

Conséquence: tout élément de $\mathbb{F}_q$ est somme de 2 carrés.

3 Polynômes sur les corps finis

$\mathbb{F}_q$: corps fini; n: entier $\geqslant 1$.

3.1 Existence de polynômes irréductibles

Soit α générateur de $\mathbb{F}_{q^n}^*$. Alors $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Le polynôme minimal de α sur $\mathbb{F}_q$ est un polynôme irréductible de $\mathbb{F}_q[X]$ de degré n.

3.2 Corps de décomposition, corps de rupture

Théorème 8 *Soit f un polynôme irréductible de $\mathbb{F}_q[X]$ de degré n. Alors f a une racine $\alpha \in \mathbb{F}_{q^n}$. De plus, f a n racines simples dans $\mathbb{F}_{q^n}$: α, α^q, α^{q^2}, ..., $\alpha^{q^{n-1}}$.*

Conséquences:

Le corps de rupture et le corps de décomposition d'un polynôme irréductible sont les mêmes. Deux polynômes irréductibles de même degré ont le même corps de décomposition.

Automorphismes de $\mathbb{F}_{q^n}$ laissant $\mathbb{F}_q$ invariant: groupe engendré par $x \mapsto x^q$ (cyclique d'ordre n).

Si p est premier, n divise $\varphi(p^n - 1)$.

3.3 Théorème de Chevalley

Théorème 9 *K: corps fini de caractéristique p. Soient $f_i \in K[X_1, \ldots, X_n]$ des polynômes à n variables tels que $\sum \deg(f_i) < n$. Alors le nombre de zéros communs dans K^n est divisible par p.*

Corollaire 1 *Si les f_i sont sans terme constant, alors ils ont un zéro commun non trivial.*

4 Applications

4.1 Groupes simples finis

$PSL(n, K)$ est simple sauf pour $n = 2$ et $K = \mathbb{F}_2$ ou $\mathbb{F}_3$. De plus, si K est fini, $PSL(n, K)$ est un groupe simple fini.

4.2 Théorème de Sylow

Lemme 1 *L'ensemble des matrices triangulaires supérieures dont les termes diagonaux sont égaux à 1 est un p-sous-groupe de Sylow de $GL(\mathbb{F}_p^n)$.*

4.3 Construction de matrices de Hadamard

Matrices de Hadamard H_n: matrices de $\mathcal{M}_{n,n}(\{\pm 1\})$ telles que $H_n H_n^{\mathrm{T}} = nI_n$.

Théorème 10 *Soient a_1, ..., a_q les éléments de $\mathbb{F}_q$ avec $q \equiv 3 \bmod 4$, η le caractère quadratique de $\mathbb{F}_q$, et $H = (b_{ij})_{0 \leqslant i,j \leqslant q}$ avec $b_{ij} = +1$ pour $i = 0$ ou $j = 0$, $b_{ij} = -1$ pour $i = j \geqslant 1$, $b_{ij} = \eta(a_j - a_i)$ pour $i, j \geqslant 1$ et $i \neq j$. Alors H est une matrice de Hadamard d'ordre $q + 1$.*

4.4 Codes linéaires

Alphabet fini: $\mathbb{F}_q$ (en général $q = 2$). Codage: $\mathbb{F}_q^k \to \mathbb{F}_q^n$. Soient $A \in \mathcal{M}_{n-k,k}(\mathbb{F}_q)$ et $H = (A, I_{n-k})$. Message $a_1 a_2 \cdots a_k \mapsto c = a_1 \cdots a_k c_{k+1} \cdots c_n$ avec $Hc^{\mathrm{T}} = 0$; c_i: symboles de contrôle. $C = \mathrm{Im}(\mathbb{F}_q^k)$.

$d_C = \min\{w(c) : c \in C \backslash \{0\}\}$ où $w(c)$ est le nombre de composantes non nulles; $d_C \geqslant s + 1$ ssi s colonnes de H sont toujours linéairement indépendantes. C peut corriger jusqu'à t erreurs si $d_C \geqslant 2t + 1$.

Code cyclique: linéaire et stable par permutations circulaires. C est cyclique ssi C est un idéal de $\mathbb{F}_q[X]/(x^n - 1)$.

Références

Serre: Cours d'arithmétique.
Lidl: Introduction to finite fields and their applications.
Menezes: Application of finite fields.
Perrin.