Corps finis. Applications

123

[Perrin]

Motivations : Cryptographie / Transformée de Fourier discrète / Codes correcteurs.

I Corps finis

1) Construction des corps finis

K est un corps.

Def 1 : La caractéristique de K est le générateur de $\ker \varphi$ où $\varphi : \mathbb{Z} \to K$, $n \mapsto n.1 = \underbrace{1+1+\dots+1}_{n \text{ fois}}$. On notera $\mathrm{char}(K)$

Prop 2 : La caractéristique d'un corps K est nulle ou un entier p premier.

Prop 3 : $\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff$ n est premier

Ex 4 : $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p / $\mathbb{Q}$ est de caractéristique 0

Def/prop 5 : Le sous corps premier de K est le plus petit sous corps de K (contenant 1). Il vaut $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ si $\mathrm{char}(K) = p$ / $\mathbb{Q}$ si $\mathrm{char}(K) = 0$

Ex 6 : $\mathbb{F}_p(X)$ a pour sous corps premier $\mathbb{F}_p$
$\mathbb{R}$ et $\mathbb{C}$ ont pour sous corps premier $\mathbb{Q}$.

Corollaire 7 : Tout corps fini K est une extension de $\mathbb{F}_p$
Si $n = \dim_{\mathbb{F}_p}(K) = [K : \mathbb{F}_p]$, alors $|K| = p^n$

Def 8 : Le morphisme de Frobenius est $F : K \to K$, $x \mapsto x^p$ pour $p = \mathrm{char}(K)$

Prop 9 : F est un automorphisme (pour K fini), injectif + même cardinal au départ et à l'arrivée.
F est l'identité sur $\mathbb{F}_p$ (petit théorème de Fermat)

Ex 10 : Pour tout x dans $\mathbb{F}_7$, $x^7 = x$.

Thm Def 11 : Soit $q = p^n$, il y a existence et unicité à isomorphisme (non unique) près du corps à q éléments. On le note $\mathbb{F}_q$.
- $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$
- $\mathbb{F}_q$ est l'ensemble des racines de $X^q - X$ sur une clôture algébrique de $\mathbb{F}_p$

Prop 12 : Soit P un polynôme irréductible de degré n sur $\mathbb{F}_p$. Le corps $\mathbb{F}_q$ est alors le corps de rupture de P sur $\mathbb{F}_p$

Ex 13 : $\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{(X^2+X+1)}$ cf. annexe Attention $\mathbb{F}_4 \not\simeq \mathbb{Z}/4\mathbb{Z}$

Prop 14 : On a $(\mathbb{F}_q, +) \simeq (\mathbb{Z}/p\mathbb{Z})^n$ en tant que groupe abélien fini

Ex 15 : $\mathbb{F}_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Thm 16 : On a $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ si et seulement si $n \mid m$

Ex 17 : Diagramme d'inclusions pour p = 2 en annexe

[NH2G2]

2) Dénombrement et géométrie sur les corps finis

→ comme produit cartésien d'ensemble fini : $|(\mathbb{F}_q)^N| = q^N$

→ en faisant agir $\mathbb{F}_q^*$ sur $(\mathbb{F}_q)^{n+1} \setminus \{0\}$: $|\mathbb{P}^n(\mathbb{F}_q)| = 1 + q + \dots + q^n$

→ en comptant les bases de $(\mathbb{F}_q)^n$: $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1})$

→ en quotientant $GL_n(\mathbb{F}_q)$ par les homothéties $|PGL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}$

→ en utilisant le morphisme déterminant : $|SL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}$

→ en quotientant $SL_n(\mathbb{F}_q)$ par son centre : $|PSL_n(\mathbb{F}_q)| = \frac{1}{\mathrm{pgcd}(q-1,n)} |SL_n(\mathbb{F}_q)|$

car $|\mu_n(\mathbb{F}_q)| = \mathrm{pgcd}(q-1, n)$

Prop 18 : On a les isomorphismes exceptionnels suivants :

(i) $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_2) \simeq PGL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$

(ii) $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$, $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$

(iii) $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$

(iv) $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$, $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$

[Perrin]

3) Etude des carrés sur les corps finis

Def 19 : $\mathbb{F}_q^2$ est l'ensemble des carrés de $\mathbb{F}_q$: $\{x \in \mathbb{F}_q \mid \exists a \in \mathbb{F}_q \; x = a^2\}$
$\mathbb{F}_q^{*2}$ est l'ensemble des carrés de $\mathbb{F}_q^*$: $\{x \in \mathbb{F}_q^* \mid \exists a \in \mathbb{F}_q^* \; x = a^2\}$

Ex 20 : Les carrés de $\mathbb{F}_7^*$ sont 1, 2 et 4

Prop 21 : $\mathbb{F}_q^*$ et $\mathbb{F}_q^{*2}$ sont des groupes cycliques

Rmq 22 : En pratique, il n'est pas facile de trouver un générateur de ces groupes [Perrin] [Dem]

Ex 23 : 2 est un générateur de $(\mathbb{Z}/11\mathbb{Z})^*$

$\bar{X}$ est un générateur de $(\mathbb{F}_4)^*$

4 est un générateur de $(\mathbb{Z}/11\mathbb{Z})^{*2}$

Prop 24 : Pour $p>2$, x est un carré dans $\mathbb{F}_q^* \iff x^{\frac{q-1}{2}} = 1$

Corollaire 25 : -1 est un carré dans $\mathbb{F}_q \iff q \equiv 1 [4]$

Application 26 : Théorème des deux carrés (cas p premier)

Application 27 : Classification des formes quadratiques sur $\mathbb{F}_q$ par le discriminant

Def 28 : Le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut $\begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p \\ 0 & \text{si } a=0 \\ -1 & \text{sinon} \end{cases}$

Ex 29 : $\left(\frac{-1}{3}\right) = -1$ et $\left(\frac{2}{7}\right) = 1$

Prop 30 : pour a,b entiers on a $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} [p]$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ [Dem]

$\left(\frac{-1}{p}\right) = 1$ ssi $p \equiv 1 [4]$ $\quad \left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 [3] \\ -1 & \text{si } p \equiv 2 [3] \end{cases}$

Thm 31 : Loi de réciprocité quadratique

Soient p,q premiers impairs distincts, on a $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$ DEV 1

II) Irréductibilités des polynômes sur $\mathbb{F}_q[X]$

La connaissance d'un polynôme irréductible de degré n sur $\mathbb{F}_p$ valide la construction alternative de $\mathbb{F}_q$ proposée en 12

a) Critère d'irréductibilité

Prop 32 : Soit $P \in \mathbb{F}_q[X]$ de degré n. P est irréductible sur $\mathbb{F}_q$ si et seulement si P n'a pas de racine dans les extensions de $\mathbb{F}_q$ de degré inférieur ou égal à $n/2$ [Perrin]

Ex 33 : Pour montrer que X^4+X+1 est irréductible sur $\mathbb{F}_2$, il suffit de montrer qu'il n'a pas de racine dans $\mathbb{F}_2$ ni $\mathbb{F}_4$

Prop 34 : Soit $P \in \mathbb{F}_q[X]$ irréductible de degré n, soit K une extension de degré m avec $\text{pgcd}(m,n)=1$. Alors P est irréductible sur K

Ex 35 : X^3+X+1 n'a pas de racines dans $\mathbb{F}_2$, donc est irréductible sur $\mathbb{F}_{2^n}$ si $3 \nmid n$. Par contre il est réductible sur $\mathbb{F}_8$.

Prop 36 : (critère d'Eisenstein) Soit $P = a_nX^n + \dots + a_1X + a_0 \in \mathbb{Z}[X]$, on suppose qu'il existe p premier tel que

(i) $\forall 0 \leq k \leq n-1$ $p \mid a_k$ (ii) $p \nmid a_n$ (iii) $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$ [Gou]

Ex 37 : $P(X) = X^4+1$ est irréductible sur $\mathbb{Z}$ car $P(X+1)$ l'est avec $p=2$

Prop 38 : Soit $P \in \mathbb{Z}[X]$, soit p premier, on pose $\bar{P}$ la réduction de P dans $\mathbb{F}_p[X]$, on suppose que $\bar{a}_n \neq 0$. Alors, si $\bar{P}$ est irréductible dans $\mathbb{F}_p[X]$, on a P irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$ [Perrin]

Ex 39 : $P(X) = X^3+4X^2-5X+7 \equiv X^3+X+1 [2]$ irréductible sur $\mathbb{F}_2$

Donc P est irréductible sur $\mathbb{Z}$

Réciproque fausse 40 : X^4+1 est réductible sur tous les $\mathbb{F}_p$ mais irréductible sur $\mathbb{Z}$.

2) Les polynômes cyclotomiques

Intérêt 41 : étude des irréductibles de X^N-1 sur $\mathbb{F}_q$

On fixe N et $q = p^n$ tels que $\text{pgcd}(N,p) = 1$

Def 42 : On considère $K_{N,p}$ le corps de décomposition de X^N-1 sur $\mathbb{F}_p$. On pose $\Phi_{N,p}(X) = \prod_{\omega \in \mu_N^*(K_{N,p})} (X-\omega)$

où $\mu_N^*(K_{N,p})$ est l'ensemble des racines primitives N-ièmes de l'unité sur $K_{N,p}$

Ce sont les polynômes cyclotomiques [Perrin]

Ex 43 : $\Phi_{2,3}(X) = X+1$ car $\mu_2^*(K_{2,3}) = \{-1\}$

Prop 44 : On a $X^N - 1 = \prod_{d \mid N} \Phi_{d,p}(X)$

Utilisation 45 : On peut calculer les polynômes cyclotomiques récursivement grâce à cette propriété voir annexe.

Prop 46 : On suppose $\text{pgcd}(N,q) = 1$ ($\iff p \nmid N$). Soit r l'ordre de q dans le groupe $(\mathbb{Z}/N\mathbb{Z})^*$. Alors $\Phi_{N,p}$ se décompose dans $\mathbb{F}_q[X]$ en produit de polynômes irréductibles, de degré r, tous différents. [Pey]

3) Déterminer automatiquement si un polynôme est irréductible

Algo. 47. Algorithme de Berlekamp
Cet algorithme permet de trouver la décomposition en facteurs irréductibles d'un polynôme sur $\mathbb{F}_q$.

DEV 2 Max

III Applications au monde réel

1) Trouver des nombres premiers très très grands

Def 48: Un nombre de Mersenne s'écrit $2^q - 1$ pour q premier impair. On le note M_q.

Thrm 49: M_q premier $\iff (2+\sqrt{3})^{2^{q-1}} \equiv -1 [M_q]$

DEV 2 Pierre

Algo 50: Test de Lehmer Lucas
Soit $(L_n)_{n\geq 0}$ la suite de $\mathbb{Z}/M_q\mathbb{Z}$ définie par $L_0 = 4$ et $L_{n+1} = L_n^2 - 2 [M_q]$
Alors M_q premier $\iff L_{q-2} \equiv 0 [M_q]$

Appli 51: → Système RSA.
→ Donne le plus grand nombre premier qu'on connaisse

2) Transformée de Fourier Rapide (TFR)

Def 52: (Transformée de Fourier Discrète TFD) Soit $N \in \mathbb{N}^*$
Pour ω une racine $N^{\text{ième}}$ primitive de l'unité dans $\mathbb{F}_q$ on pose $\mathcal{F}: \begin{array}{l} (\mathbb{F}_q)^N \to (\mathbb{F}_q)^N \\ (a_i)_1^N \mapsto \left(\sum_{k=0}^{N-1} a_k \omega^{-kj}\right)_{j=1}^N \end{array}$ la TFD

et $\overline{\mathcal{F}}: \begin{array}{l} (\mathbb{F}_q)^N \to (\mathbb{F}_q)^N \\ (a_i)_1^N \mapsto \left(\sum_{k=0}^{N-1} a_k \omega^{kj}\right)_{j=1}^N \end{array}$ la TFD inverse

Prop 53: On a $\mathcal{F}(\overline{\mathcal{F}}(a)) = Na$ et $\overline{\mathcal{F}}(\mathcal{F}(a)) = Na$ $\forall a \in (\mathbb{F}_q)^N$

Prop 54: (Convolution) $\mathcal{F}(a * b) = \mathcal{F}(a).\mathcal{F}(b)$ et $\overline{\mathcal{F}}(a * b) = \overline{\mathcal{F}}(a).\overline{\mathcal{F}}(b)$ avec $a.b$ le produit terme à terme de a et b $(a,b \in (\mathbb{F}_q)^N)$

Prop 55: (TFR) Étant donnée une racine primitive $N^{\text{ième}}$ de l'unité dans $\mathbb{F}_q$, on peut calculer récursivement la TFD en $\mathcal{O}(N \log N)$

Appli 56: Multiplication des grands polynômes/grands entiers en $\mathcal{O}(N \log N)$ (schéma en annexe)

3) Codes correcteurs

Def 57: Un code linéaire C de taille N et de dimension m est un sous espace vectoriel de dimension m de $(\mathbb{F}_q)^N$.

Def 58: Un code linéaire est cyclique s'il est stable par décalage circulaire (i.e. si $a_0 \dots a_{n-1} \in C$ alors $a_{n-1} a_0 a_1 \dots a_{n-2} \in C$)
On peut le voir comme multiplication par X via l'isomorphisme $\begin{array}{l} (\mathbb{F}_q)^N \xrightarrow{\sim} \mathbb{F}_q[X]/(X^N - 1) \\ (a_i)_0^{N-1} \mapsto \sum_{i=0}^{N-1} a_i X^i \end{array}$, ainsi C est stable par multiplication par tout polynôme donc c'est un idéal de $\mathbb{F}_q[X]/(X^N - 1)$, il est isomorphe à un idéal (principal) de $\mathbb{F}_q[X]$ contenant $X^N - 1$ (par la correspondance des idéaux)
Donc un code cyclique est engendré par un unique facteur irréductible P de $X^N - 1$ sur $\mathbb{F}_q$.

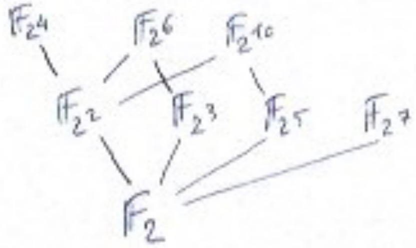
Ex 59: Les codes BCH utilisent la cyclotomie pour générer des codes de distance minimale fixée. Leur décodage s'effectue efficacement par TFR.

[Dem] [Sau] [Dem] [Pey] [Dem] [Pey] [Sau]

Annexe 1 : table de $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(1+X+X^2)$ multiplicative

	0	1	$\bar{X}$	$1+\bar{X}$
0	0	0	0	0
1	0	1	$\bar{X}$	$1+\bar{X}$
$\bar{X}$	0	$\bar{X}$	$1+\bar{X}$	1
$1+\bar{X}$	0	$1+\bar{X}$	1	$\bar{X}$

Annexe 2 : Diagramme des inclusions des $\mathbb{F}_{2^k}$



Annexe 4 : $N = 2^n \quad N \geqslant \deg P + \deg Q + 1$

$$\begin{tikzcd}
(P,Q) \in \mathbb{F}_q^N \times \mathbb{F}_q^N \arrow[r, "TFR_\omega", "G(N\log N)"'] & (\mathcal{F}P, \mathcal{F}Q) \in \mathbb{F}_q^N \times \mathbb{F}_q^N \arrow[d, "G(N)"', "\text{produit terme à terme}"] \\
(P \times Q) \in \mathbb{F}_q^N & \mathcal{F}P . \mathcal{F}Q = \mathcal{F}(P * Q) \arrow[l, "G(N\log N)"', "TFR_{\omega^{-1}}"]
\end{tikzcd}$$

Annexe 3 : pour $p = 11$

n	$\Phi_{n,p}(X)$
1	$X-1$
2	$X+1$
3	X^2+X+1
4	X^2+1
5	$X^4+X^3+X^2+X+1$
6	X^2-X+1
7	$X^6+X^5+X^4+X^3+X^2+X+1$
8	X^4+1

Références :

[Per] Daniel Perrin, Cours d'algèbre

[Pey] Gabriel Peyré, L'algèbre discrète de la transformée de Fourier

[Sau] Saux Picart-Rannou, Cours de calcul formel, corps finis systèmes polynomiaux applications

[NH2G2] Caldero-Germoni NH2G2 Tome 2

[Dem] Michel Demazure, Cours d'algèbre

[Gou] Xavier Gourdon, Algèbre