

Cadre V est un autre premier, $q = p^2$ ou non premier

1. Construction de $\mathbb{F}_q$

1. Structure de base

Def 1. On appelle corp. fini tout corp. de cardinal fini

Prop 1. Soit K un corp. fini

(1) Soit n cardinalité de K (logique K est $\mathbb{F}_q$)

(2) K est muni d'une structure de $\mathbb{F}_p$ -espace vectoriel

Coroll 1. $|K| = p^n$ ou $n \in \mathbb{N}$

Prop 2. Soit $K \in \mathbb{F}_p[x]$ est une suite de K , de degré d
 et $\langle K \rangle$ est un corp. de cardinal p^d

Ex 1. $p=2$, $\mathbb{F}_2[x]$ est un corp. de cardinal 4 : c'est $\{0, 1, x, x+1\}$
 $\langle x^2+x+1 \rangle$

Ex 2. Une $\mathbb{F}_p$ -base de K est $\{1, x, \dots, x^{d-1}\}$, et K est la somme de x modules $\langle p \rangle$

Def 3. On définit la multiplication de Frobenius par

$$\begin{aligned} \sigma: K &\rightarrow K \\ x &\mapsto x^p \end{aligned}$$

Prop 3. $\sigma \in \text{Aut}(K)$

Prop 4. $\forall x \in K$, $\sigma(x^{p^k}) = x^{p^{k+1}}$ est un auto-corp. de K

Prop 5. $\text{Aut}(K)$ est cyclique, engendré par le Frobenius

Ex 3. Soit $K = \mathbb{F}_2[x]$, alors $\sigma(x) = x+1$
 $\langle x^2+x+1 \rangle$ $\sigma(x+1) = x$

Donc $\text{Aut}(K) = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$

Th 1. Un corp. fini K de cardinal $q = p^n$ est isomorphe à

$\mathbb{F}_p$ est corp. de décomposition en $\mathbb{F}_p$ de $X^{p^n} - X$

En particulier, $\mathbb{F}_p$ est unique à isomorphisme près

Ex 4. On note $\mathbb{F}_q$ est unique $\mathbb{F}_q = \mathbb{F}_{p^n}$

Ex 5. $\mathbb{F}_q = \frac{\mathbb{F}_p[x]}{\langle x^n-1 \rangle}$

2. Structure de corps multiplicatif

Prop 6. Pour tout corp. fini K , son groupe de multip. K^* est cyclique. Si $|K|=q$, alors $K^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$

Ex 6. $\mathbb{F}_3 = \frac{\mathbb{F}_2[x]}{\langle x^2+x+1 \rangle}$, alors $\mathbb{F}_3^*$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$

Prop 7. Si α est racine $\mathbb{F}_q^*$, alors $\mathbb{F}_q = \mathbb{F}_p[\alpha]$

Ex 7. $\mathbb{F}_4$ engendré α^2 , et $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$

Th 2. (Théorème de l'élément primitif)

Soit K un corp. fini. Soit k une extension de degré fini de K

Alors $\exists \gamma \in K$: $k = K(\gamma)$ γ est appelé élément primitif de k

Ex 8. $\mathbb{F}_4$ est élément primitif de $\mathbb{F}_4$

Prop 8. Si γ est un élément primitif de $\mathbb{F}_q$ alors $\gamma, \gamma^2, \dots, \gamma^{q-2}$
 est une $\mathbb{F}_p$ -base de $\mathbb{F}_q$ en $\mathbb{F}_p$

3. Sous-corps d'un corp. fini

Th 3. (Théorème de la base d'extension)

Soit K un corp. fini, $L \subset K$ un sous corp. Soit E un $\mathbb{F}_p$ -espace vectoriel de base $\{e_i\}$, et $\sigma \in \text{Aut}(K)$. Soit $\{f_j\} \subset K$ une base de L en tant que $\mathbb{F}_p$ -espace vectoriel. Alors

$\{e_i f_j\}$ est une base de E en tant que $\mathbb{F}_p$ -espace vectoriel

Si L est un corp. fini, et $\dim_{\mathbb{F}_p}(L) = n$, alors

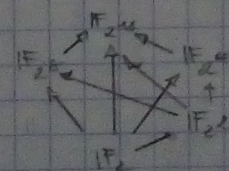
$$\dim_{\mathbb{F}_p}(L) = \dim_{\mathbb{F}_p}(E) \cdot [L:K]$$

Prop 9. $X^{p^n} - X \mid X^{p^m} - X$ si et seulement si $n \mid m$

Prop 10. Il existe un unique corp. de $\mathbb{F}_{p^n}$ de p^d éléments
 où $d \mid n$

Ex 9. Isomorphisme de sous-corps de $\mathbb{F}_{2^4}$

→ sous-corps de



I - Corps finis et polynômes

1 - Caractérisation de corps des deux types

Prop 25. F_q / F_p est fini, donc abélien, donc tout élément non nul d'un polynôme minimal irréductible sur F_p .

Th 26. Soit ζ un élément primitif de F_q sur F_p son polynôme minimal est $F_q \simeq \frac{F_p[X]}{\langle \mu_\zeta \rangle}$ ou $n = \deg(\mu_\zeta)$.
On a même les isomorphismes

$$\text{car } \zeta : \frac{F_p[X]}{\langle \mu_\zeta \rangle} \xrightarrow{\sim} F_q$$

$$X \mapsto \zeta$$

Prop 29. Si $P \in F_p[X]$ est irréductible de degré d , alors $\frac{F_p[X]}{\langle P \rangle}$ est un corps à p^d éléments.

Ex 28. X est élément primitif de $\frac{F_p[X]}{\langle P \rangle}$, où P est un polynôme irréductible. $\{X, X^2, \dots, X^{p^d-1}\}$ est une F_p -base de $\frac{F_p[X]}{\langle P \rangle}$ car F_p -espace vectoriel de dimension d .

Ex 29. $P = X^2 + X + 1$ est irréductible dans $F_2[X]$.

$\frac{F_2[X]}{\langle P \rangle}$ est un corps C est un F_2 -es de dimension 2 sur F_2 .
 $\langle X^2 + 1 \rangle$

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

Les tables d'addition et de multiplication sont données par :

+	0	1	X	X+1
0	0	1	X	X+1
1	1	0	X+1	X
X	X	X+1	0	1
X+1	X+1	X	1	0

x	0	1	X	X+1
0	0	0	0	0
1	0	1	X	X+1
X	0	X	X+1	1
X+1	0	X+1	1	X

2 - Polynômes irréductibles sur F_q

Prop 30. $F_q \simeq \frac{F_p[X]}{\langle P \rangle}$ où P est le polynôme minimal d'un élément primitif de F_q sur F_p .

Ex 31. Il existe deux des polynômes irréductibles de degré 2 sur $F_2[X]$, ce qui est facile par les deux info.

Ex 32. Soit $P \in F_q[X]$ un polynôme de degré d sur F_q .

Prop 33. Si P est un polynôme irréductible de degré d sur F_q et $P \mid X^{q^n} - X$ dans $F_q[X]$, les éléments de F_{q^n} sont les racines de P dans F_{q^n} .

Def 34 (Générateur de l'extension). On définit la fonction de l'extension μ par :

$$\begin{cases} \mu(1) = 1 \\ \mu(a) = a^{q^n} - a \text{ si } a \text{ est un élément de } F_{q^n} \\ \mu(a) = 0 \text{ si } a \text{ est un élément de } F_{q^n} \end{cases}$$

Th 35. Le nombre de polynômes irréductibles unitaires de degré n sur F_q est

$$I(n, q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$$

$$\text{ou } I(n, q) \sim \frac{q^n}{n}$$

DWPT-1

Prop 36 (Fonction de Moebius)

Soit $P \in F_q[X]$, écrit sa décomposition en irréductibles est sous forme canonique

$$P = \prod_{i=1}^r P_i^{e_i}$$

Le nombre de facteurs irréductibles de P est

DWPT-2

$$\delta = \dim(\ker(S_p - Id)) \text{ où } S_p : \frac{F_p[X]}{\langle P \rangle} \rightarrow \frac{F_p[X]}{\langle P \rangle}$$

$$\overline{\phi} \mapsto \overline{\phi}^p$$

(i) $\exists \overline{v} \in \ker(S_p - Id)$ alors comme modulo P a un polynôme constant de $F_q[X]$ à $P = \prod_{i=1}^r \text{Irr}(P, v_i, x)$ sur F_q .

App 4.33. Polymère d'un pyrène P_6H_6 [1]

III - Genes de Fe

Page 23 Sub to E.P.

$$\text{Prob } \overline{xy} \in \mathbb{F}_p \quad x = y^2 \iff x = \frac{p+1}{2} = 1$$

Ex 40 7 vult ao gas um nome do IF_{11}

$$= \frac{1}{\sqrt{6}} \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} \right) = 0$$

Exercice 42: (Symbole de Legendre) Soit $n \in \mathbb{Z}$. On pose:

$$\left(\frac{n}{3}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{3} \\ 0 & \text{if } n \equiv 2 \pmod{3} \\ -1 & \text{if } n \equiv 0 \pmod{3} \end{cases}$$

Se $\left(\frac{m}{n}\right) = 1$, então m é um número quadrado.

Prop 42 8 p 73

$$\frac{1}{2} \left(\frac{1}{2} \right) = \frac{1}{4}$$

$$\left(\begin{array}{c} 1 \\ 0 \\ 0 \end{array} \right) = \left(\begin{array}{c} 1 \\ 1 \\ 2 \end{array} \right) + \left(\begin{array}{c} 0 \\ -1 \\ -2 \end{array} \right)$$

Th 43: Loi de Laplace quelconque

Sono P ed P' due entità differenti; $P \wedge P' = 1$

$$\left(\frac{p}{p'}\right) = \left(\frac{p'}{p}\right) (-1)^{\frac{p-1}{2}(p'-1)}$$

$$\text{b) } - \left(\frac{-1}{0} \right) = (-1) \frac{1-1}{2}$$

$$(1) \quad \left(\frac{2}{1} \right) = (-1) \quad \frac{b^2 - 4}{4}$$

$$\begin{aligned} a, \quad \left(\frac{-1}{-1} \right) &= \left(\frac{24}{-12} \right) = \left(\frac{2}{-1} \right) \left(\frac{-4}{-10} \right) = (-1) \left(\frac{-2}{5} \right) (-1) \\ &= (-1) \left(\frac{2}{5} \right) (-1) = (-1) \left(\frac{2}{5} \right) (-1) = \left(\frac{2}{5} \right) \\ &= \left(\frac{2}{5} \right) (-1) = \left(\frac{2}{5} \right) (-1) = - \left(\frac{2}{5} \right) = -1 \end{aligned}$$

References

IT. P. Serie, Cours d'Acoustique

D. Proust, Cours d'algèbre