Corps finis. Applications

123

I/ Structure

1) Caractéristique et génération

Prop 1: Soit F un corps fini
- Sa caractéristique est un nombre premier p
- Son sous-corps premier est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
- F est un $\mathbb{F}_p$-ev, et si $n = [F:\mathbb{F}_p]$, $|F| = p^n$

C-ex 2: Il n'existe pas de corps à $221 = 13 \times 17$ éléments

th 3 (Wedderburn): Toute algèbre à division finie est un corps

th 4: le groupe des inversibles d'un corps fini est cyclique

Ex 5: générateurs de $\mathbb{F}_p$

p	3	5	7	11	13	17	23
g	2	2	3	3	6	7	5

Prop 6: Soit F corps fini de caractéristique p, et ξ un générateur de $\mathbb{F}^*$. Alors $F = \mathbb{F}_p(\xi) = \mathbb{F}_p[\xi]$, et si $n = [F:\mathbb{F}_p]$, $F = \mathbb{F}_p \oplus \xi\mathbb{F}_p \oplus \cdots \oplus \xi^{n-1}\mathbb{F}_p$

C-ex 7: X^2+1 est irréductible sur $\mathbb{F}_7$. Soit α une racine de celui-ci dans $\mathbb{F}_7[X]$ / alors $\mathbb{F}_7[X]/(X^2+1) = \mathbb{F}_7(\alpha)$, mais α n'engendre pas $\mathbb{F}_7(\alpha)^* = \langle X^2+1 \rangle$

th 8: Elément primitif
Toute extension L de degré fini d'un corps fini K est monogène : $\exists \xi \in L$ tel que $L = K(\xi)$

2) Existence et unicité de $\mathbb{F}_{p^n}$, automorphismes

Déf-prop 9: Endomorphisme de Frobenius.
Si F est un corps de caractéristique p, $x \mapsto x^p$ est un endomorphisme de F, appelé endomorphisme de Frobenius de F
- Si $F = \mathbb{F}_p$, $\mathcal{F} = Id$
- Si F est fini, $\mathcal{F}$ est un automorphisme de F

Corollaire 10: petit théorème de Fermat
Soit p premier. Alors $\forall k \in \mathbb{Z}$, $k^p \equiv k\ [p]$

Cor 11: Dans un corps de caractéristique p, tout élément admet une unique racine p-ième.

th 12: Soit p premier, $n \in \mathbb{N}^*$, $q = p^n$
À $\mathbb{F}_p$-isomorphisme près, $\exists!$ corps à q éléments, noté $\mathbb{F}_q$
C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Cor 13: $\prod_{a \in \mathbb{F}_p^*} a = -1$

th 14: le groupe des $\mathbb{F}_p$-automorphismes de $\mathbb{F}_q$ est cyclique, d'ordre n, engendré par $\mathcal{F}$

3) A l'intérieur

th 15: p premier, $n \in \mathbb{N}^*$, $q = p^n$. Les sous-groupes additifs de $\mathbb{F}_q$ sont ses sous $\mathbb{F}_p$-espaces vectoriels
Ils sont au nombre de $\sum_{s=0}^{n} \frac{(p^n-1)\cdots(p^{n-s+1}-1)}{(p^s-1)\cdots(p-1)}$

th 16: K est un sous corps de $\mathbb{F}_q \Rightarrow \exists d \mid n$ tel que $\mathrm{Card}(K) = p^d$.
- $\forall d \mid n$, $\exists!$ sous corps de $\mathbb{F}_q$ de cardinal p^d, c'est $\{x \in \mathbb{F}_q,\ x^{p^d} = x\}$

Corollaire 17: $\mathbb{F}_q$ sous corps de $\mathbb{F}_{q'} \Leftrightarrow q$ est une puissance de q.

Exemple 18: Sous corps de $\mathbb{F}_{4096}$ en annexe

II/ Carrés d'un corps fini

1) L'objet

Déf-Prop 19: p premier, $n \in \mathbb{N}^*$, $q = p^n$. On pose
$\mathbb{F}_q^{\square} = \{x^2,\ x \in \mathbb{F}_q\}$, $\mathbb{F}_q^{*\square} = \mathbb{F}_q^{\square} \cap \mathbb{F}_q^*$
$\mathbb{F}_q^{*\square}$ est un sous-groupe de $\mathbb{F}_q^*$

Prop 20 : - Si $p=2$, $\mathbb{F}_q^{*\square} = \mathbb{F}_q$ (par 7), $\mathbb{F}_q^{*\square} = \mathbb{F}_q^*$

- Si $p > 2$

(i) $x \mapsto x^2$ a pour noyau $\{-1, 1\}$. En tant que son image, $\mathbb{F}_q^{*\square}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^*$.

$|\mathbb{F}_q^{*\square}| = \frac{q-1}{2}$

(ii) $\mathbb{F}_q^{*\square}$ est le noyau de $x \mapsto x^{\frac{q-1}{2}}$

(iii) $-1 \in \mathbb{F}_q^{*\square} \iff q \equiv 1 [4]$

Prop 21 : (iii) implique que si -1 n'est pas un carré dans $\mathbb{F}_q$, il l'est dans $\mathbb{F}_{q^2} = 3^2 = 9 \equiv 1 [4]$.

On pouvait aussi voir que $\mathbb{F}_{q^2}$ est alors corps de rupture du polynôme irréductible x^2+1

Corollaire (de (iii)) 22 :

Il existe une infinité de nombres premiers de la forme $4k+1$

2) Symbole de Legendre : Soit p premier impair

Déf 23 : On définit le symbole de Legendre sur $\mathbb{F}_p$ par $\left(\frac{x}{p}\right) = \begin{cases} 0 \text{ si } p \mid x \\ 1 \text{ si } x \in \mathbb{F}_p^{*\square} \\ -1 \text{ sinon} \end{cases}$

Prop 24 : $\forall x \in \mathbb{F}_p^*$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$, et $\mathbb{F}_p^* \to \{-1,1\}$, $x \mapsto \left(\frac{x}{p}\right)$ est un morphisme de groupes non constant

25 : Conséquences

- Un générateur de $\mathbb{F}_p^*$ n'est pas un carré de $\mathbb{F}_p$
- Pour calculer $\left(\frac{xy}{p}\right)$, il suffit de connaître les symboles de Legendre des facteurs premiers de x

Th 26 : Loi de réciprocité quadratique

p, q premiers impairs distincts

Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

Prop 27 : Pour p premier impair $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Ex 28 : $\left(\frac{17}{41}\right) = (-1)^{8\times 20}\left(\frac{41}{17}\right) = \left(\frac{7}{17}\right) = (-1)^{3\times 8}\left(\frac{3}{7}\right)$

$= (-1)^3\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1 : 17 \notin \mathbb{F}_{41}^{*\square}$

App 29 : $x^2+2x-16=0 \iff (x+1)^2 = 17$ n'a pas de solution dans $\mathbb{F}_{41}$

3) Carrés de $\mathbb{F}_q$

Déf 30 : Pour $a \in \mathbb{F}_q$ ($\mathbb{F}_q$ comme $\mathbb{F}_p$-ev), on définit $N_{\mathbb{F}_q/\mathbb{F}_p}(a)$ comme le déterminant de $x \mapsto ax$

Prop 31 : $N_{\mathbb{F}_q/\mathbb{F}_p}(a) = a^{\frac{q-1}{p-1}} \in \mathbb{F}_p$

Prop 32 : a est un carré de $\mathbb{F}_q \iff$ $N_{\mathbb{F}_q/\mathbb{F}_p}(a)$ est un carré de $\mathbb{F}_p$.

Prop 33 : On ramène ainsi l'étude des carrés de $\mathbb{F}_q$ à celle des carrés de $\mathbb{F}_p$

III / Sur $\mathbb{F}_q$

1) Polynômes irréductibles, factorisation

Prop 34 : Soit q puissance de p premier, $q' = q^n$.
Si $\langle \xi \rangle = \mathbb{F}_{q'}^*$, $\pi = \mathrm{in}(\xi, \mathbb{F}_q)$ est un polynôme irréductible de $\mathbb{F}_q$ de degré $[\mathbb{F}_{q'} : \mathbb{F}_q] = n$:
Il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_q$.

Comptons les :

th 35 : Soit $q = p^n$. Pour $d \in \mathbb{N}^*$, on note $K(q,d)$ l'ensemble des polynômes irréductibles de degré d sur $\mathbb{F}_q$. On a alors $X^q - X = \prod_{d \mid n} \prod_{P \in K(q,d)} P(X)$

Cor 36 : Si $I(q,d) = |K(q,d)|$, on a $q^n = \sum_{d \mid n} d\, I(q,d)$

Cor 37 : $I(q,n) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d \underset{n}{\sim} \frac{q^n}{n}$
où μ désigne la fonction de Möbius

th 38 : réduction modulo p
Soit $P \in \mathbb{Z}[X]$, $\overline{P}$ son image dans $\mathbb{F}_p[X]$.
Si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, P l'est dans $\mathbb{Q}[X]$

Factorisation :

th 39 : Algorithme de Berlekamp.
Pour $P \in \mathbb{F}_q[X]$ sans facteur carré, cet algorithme donne les facteurs irréductibles de P OVPT 1

lemme 40 : • $P \in D(P, P') = 1 \Leftrightarrow P$ sans facteur carré
• $P \in D(P,P') = P \Leftrightarrow \exists R \in \mathbb{F}_q[X]$, $P = R^p$
• sinon, $P \in D(P,P')$ et $\frac{P}{P \wedge D(P,P')}$ sont deux facteurs non triviaux de P

On déduit du lè 40 et de l'algorithme de Berlekamp un algorithme général de factorisation dans $\mathbb{F}_q[X]$

2) Groupe linéaire

th 41 : $|GL_n(\mathbb{F}_p)| = (p^n - 1) \cdots (p^n - p^{n-1})$

Prq 42 : $|GL_n(\mathbb{F}_p)| = p^{\frac{n(n-1)}{2}} \times m$, avec $\#\left\{\begin{pmatrix} * & * \\ (0) & q \end{pmatrix} \in GL_n(\mathbb{F}_p)\right\} = p^{\frac{n(n-1)}{2}}$. On exhibe ainsi un p-sylow de $GL_n(\mathbb{F}_p)$, et on se sert de $G \hookrightarrow S_n \hookrightarrow GL_n(\mathbb{F}_p)$ pour $|G| = n$ pour montrer l'existence d'un p-sylow de G pour $p \mid n$

th 43 : de la base normale
Pour $q = p^n$, $\exists x \in \mathbb{F}_q$ tel que $\{x, \mathcal{F}(x), \ldots, \mathcal{F}^{n-1}(x)\}$ soit une base du $\mathbb{F}_p$-ev $\mathbb{F}_q$.

th 44 : Frobenius - Zolotarev
On peut voir tout $u \in GL_n(\mathbb{F}_p)$ comme élément de S_{p^n}, et on a alors $\varepsilon(u) = \left(\frac{\det u}{p}\right)$

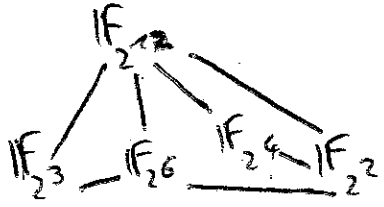
App 45 : Signature de $\mathcal{F}$: $\varepsilon(\mathcal{F}) = (-1)^{\frac{(p-1)(n+1)}{2}}$ NVPT 2

Prq 46 : Si $q \mid (p-1)(n+1)$, par exemple si p puisque $\langle \mathcal{F} \rangle = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$, $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q) \subset A_{p^n}$

Prop 47 : Si $q \neq 2^\alpha$, $SO_2(\mathbb{F}_q) \cong \begin{cases} \mathbb{Z}/(q-1)/2 & \text{si } (-1) \in \mathbb{F}_q^{*2} \\ \mathbb{Z}/(q+1)/2 & \text{sinon} \end{cases}$ □ H2G2

En particulier, $SO_2(\mathbb{F}_q)$ est alors cyclique

Annexe : Sous-corps de $\mathbb{F}_{4096} = \mathbb{F}_{2^{12}}$



$\mathbb{F}_2$ sous-corps de tous