Plan détaillé 123 Corps finis

I) Construction de corps finis ← aller voir [ROM] aussi

A) Caractéristique et extension de corps :

Déf$_{12}$: extension de corps + degré de L/K

THM$_2$: base télescopique + multip. des dl°

Déf$_3$ élément algébrique / transcendant

Déb$_4$ Corps de rupture

Ex$_5$ $\mathbb{C} = \frac{\mathbb{R}[X]}{(X^2+1)} = \mathbb{R}(i)$, $\mathbb{Q}(\sqrt{2})$: ...

THM$_6$ Existence et unicité du corps de rupture) ①

Déf$_7$ Corps de déc.

THM$_8$ Existence et unicité) ②

Déf$_9$ ss-corps 1^{er}

Déf$_{10}$ caractéristique d'un corps

Cp$_{11}$ K corps, k son sous-corps 1^{er}. Si $car(K)=0$, $k \simeq \mathbb{Q}$; si $car(K)=p$, $k \simeq \mathbb{Z}/p\mathbb{Z}$

Cq$_{12}$ $car(K) = p^n$ où p 1^{er}. Donc un corps à 6 élémt n'existe pas.

Cp-Déf$_{13}$ morphisme de Frobenius.

B) Existence – unicité (et structure) p 1^{er}, $n \in \mathbb{N}^*$, $q = p^n$

THM$_{14}$ $\mathbb{F}_q$ existe, $\mathbb{F}_q = Dec_{\mathbb{F}_p}(X^q - X)$, il est unique à isom. près

Rem$_{15}$ On a même $\mathbb{F}_q = \{$racines de $X^q - X\}$.

(*) Prop$_{16}$: sur un corps fini $\mathbb{F}_q$, $\Phi : x \mapsto x^p$ morphisme de Frob. est un automorphisme. Et $\Phi = id$ sur $\mathbb{F}_p$

THM$_{17}$ $Aut(\mathbb{F}_q)$ cyclique d'ordre n, engendré par Φ.

THM$_{18}$ · K ss corps de $\mathbb{F}_q \Rightarrow \exists\, d|n$ tq $|K| = p^d$

$\forall d|n$, $\exists$ K ss-corps de $\mathbb{F}_q$ de card p^d. C'est $K = \{x \in \mathbb{F}_q \mid x^{p^d} = x\}$

Cor$_{19}$ $d|n \Rightarrow$ on peut identifier $\mathbb{F}_{p^d}$ à l'unique ss-corps de $\mathbb{F}_q$ à p^d éléments. Donc : $\mathbb{F}_q$ ss corps de $\mathbb{F}_{q'} \Leftrightarrow q'$ puissance de q.

Rem$_{20}$ D'où le treillis d'inclusion de corps finis : $\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^4}$, $\mathbb{F}_p \subset \mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}$ ...) à mieux faire

THM$_{21}$ $\mathbb{F}_p = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$ où $\mathbb{F}_p$ = clôture algébrique de $\mathbb{F}_p$

Rem$_{22}$ D'après le thm de Steinitz, clôt. alg., unique à isom. près, mais un corps fini n'est pas alg. clos [ROM] p 426

Prop : un corps fini n'est pas alg. clos

C) Le groupe $\mathbb{F}_q^\times$:

THM$_{23}$ K corps fini. Tout ss-grpe fini de $K^\times$ est cyclique. ③

Cq$_{24}$: $\mathbb{F}_q^\times$ cyclique, $\mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

Rem$_{25}$ On ne sait pas en général trouver explicitement un générateur de $\mathbb{F}_q^\times$.

Prop$_{26}$ Thm de l'élément primitif des corps finis.

(*) Rem$_{24'}$: on peut aussi construire les corps finis à l'aide de corps de rupture, $\mathbb{F}_q = \frac{\mathbb{F}_p[X]}{(P)}$ où $P \in \mathbb{F}_p(X)$, $\deg(P) = n$, P irréductible (+ facile par faire des calculs)

(B) Ex$_{24''}$: $\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{X^2+X+1}$ d'où la table donnée en annexe + $\mathbb{F}_8$, $\mathbb{F}_9$] [GOZ] p 89

Ex$_{27}$: $\mathbb{F}_5^\times = \langle \bar{2} \rangle$, $\mathbb{F}_3^\times = \langle \bar{2} \rangle$, $\mathbb{F}_{23}^\times = \langle \bar{5} \rangle$

II) Carrés de $\mathbb{F}_q$: p 1^{er}, $n \in \mathbb{N}^*$, $q = p^n$.

A) Propriétés de $\mathbb{F}_q^2$:

Notat° 28 : $\mathbb{F}_q^2$, $\mathbb{F}_q^{\times 2}$ ...

Prop 29 : · $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$

· $p > 2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$, $|\mathbb{F}_q^{\times 2}| = \frac{q-1}{2}$, $|\mathbb{F}_q / \mathbb{F}_q^2| = \frac{q-1}{2}$.

Prop 30 ($p>2$) : $\mathbb{F}_q^{\times 2} = \{x \in \mathbb{F}_q \mid x^{\frac{q-1}{2}} = 1\}$.

Ex 31 : $q = 7$, $\frac{q-1}{2} = 3$, $\bar{2}^3 = \bar{8} = \bar{1}$ donc $\bar{2}$ est un carré de $\mathbb{F}_7$. $\bar{3}^3 = \bar{-1}$ non carré

Cor$_{32}$: $-1 \in \mathbb{F}_q^{\times 2} \Leftrightarrow q \equiv 1 [4]$.

Cor$_{33}$: $\forall a, b \in \mathbb{F}_q^*$, et $c \in \mathbb{F}_q$, $\exists x, y \in \mathbb{F}_q$ tq $c = ax^2 + y^2 b$ ④

En particulier, tout élément est somme de 2 carrés.]

Appli$_{34}$: il existe une infinité de nbre 1^{er} de la forme $4m+1$. ⑤

[PER] p. 73 [GOZ] p 83 + [PER] p 82 — [GOZ] p 58 (B) — [PER] p 83 — [GOZ] p 85 - 93 + [ROM] p 428 — 82

Plan détaillé [123] suite

II) B) Symbole de Legendre : $p \geq 3$ 1er

[PER]

Déf35 : Symbole de Legendre sur $\mathbb{F}_p^\times$

Prop36 : $\forall a \in \mathbb{F}_p^\times$, $\left|\{x \in \mathbb{F}_p^* \mid ax^2 = 1\}\right| = 1 + \left(\frac{a}{p}\right)$

THM38 : $\forall a \in \mathbb{F}_p^\times$, $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ dans $\mathbb{F}_p^*$

$\left|\begin{array}{l}\mathbb{F}_p^\times \longrightarrow \{\pm 1\} \\ a \longmapsto \left(\frac{a}{p}\right)\end{array}\right.$ est l'unique morphisme de groupe non trivial de $\mathbb{F}_p^\times \to \{\pm 1\}$

[Rom] p. 429 - 441

THM39 : Fieb - Zolotarev

Appli40 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

THM41 : Loi de réciprocité quad. (Dév 1) [CAL]

Appli42 : $\left(\frac{23}{59}\right) = -1$, $\left(\frac{17}{41}\right) = -1$ [Goz] p. 155

C) Application à la résolution d'équations polynomiales de degré 2 :

Pas de réf ...

Soit $P = aX^2 + bX + c \in K[X]$, K corps fini, $\mathrm{car}(K) \neq 2$

Déf43 : discriminant de P : $\Delta = b^2 - 4ac$

Prop44 : P admet 2 racines ($\neq$) $\Leftrightarrow \Delta \in K^{*2}$

P ___ 1 racine double $\Leftrightarrow \Delta = 0$

P n'a pas de racine $\Leftrightarrow \Delta \in K^\times \setminus K^{*2}$

Ex45 : $P = X^2 + 5X + 2 \in \mathbb{F}_{41}[X]$, $\Delta = 17 \notin \mathbb{F}_{41}^{*2}$ donc P n'a pas de racines dans $\mathbb{F}_{41}$ (P irréd. dans $\mathbb{F}_{41}$)

III) Applications :

A) Un outil pour l'irréductibilité des polynômes de $\mathbb{Z}[X]$

[PER]

Rem46 : Plonger un polynôme de $\mathbb{Z}[X]$ dans $\mathbb{F}_p[X]$ peut permettre de montrer son irréductibilité sur $\mathbb{Q}$ ou $\mathbb{Z}$.

Lemme47 : $P \in \mathbb{Z}[X]$ irréductible $\Leftrightarrow$ P irréductible sur $\mathbb{Q}[X]$ et de contenu 1.

THM48 : ~~Existe~~ Eisenstein sur $\mathbb{Z}[X]$. (6)

Appli49 : p 1er $\Phi_p = \sum_{i=0}^{p-1} X^i$ irréductible sur $\mathbb{Z}$

[PER]

THM50 : (Réduct° mod p) p 1er, $P \in \mathbb{Z}[X]$, on note $\overline{P}$ la réduction de P dans $\mathbb{F}_p[X]$ ($P = \sum_{i=0}^{n} a_i X^i$). Si $\overline{a_n} \neq \overline{0}$.
Si $\overline{P}$ irréductible dans $\mathbb{F}_p[X]$, alors P irréductible sur $\mathbb{Q}[X]$ (et sur $\mathbb{Z}[X]$ s'il est de contenu 1) (7)

Ex51 : $X^3 + 462X^2 + 2433X - 67691$ irréductible sur $\mathbb{Z}$

Prop52 : k un corps. $P \in k[X]$ de degré $n > 0$.
P irréductible sur $k \Leftrightarrow P$ n'a pas de racines dans les extensions K/k tq $[K : k] \leq n/2$

Appli53 : • $X^4 + X + 1$ irréductible sur $\mathbb{F}_2$
• $X^4 + 8X^2 + 17X - 1$ irréductible sur $\mathbb{Z}$

Rem54 : La réciproque du thm 50 est fausse : $X^n + 1$ irréductible sur $\mathbb{Z}$ mais sur aucun $\mathbb{F}_p$, p 1er.

Déf55 : polyn. cyclotomique + prop $\Phi_n = \prod_{d \mid n} \Phi_d$

THM56 : $\Phi_n \in \mathbb{Z}[X]$, irréductible.

B) Polynômes irréductibles de $\mathbb{F}_q[X]$ p 1er, $n \in \mathbb{N}^*$, $q = p^n$

[Goz] p. 87

Rem57 : On a vu que $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où $P \in \mathbb{F}_p[X]$ de d° n, irréductible, construct° utile pr les calculs donc connaître les polyn. de $\mathbb{F}_p[X]$ irréd est utile.

Lemme58 : Formule d'inversion de Möbius (+ déf μ)

[V. FRA]

THM59 : $X^q - X = \prod_{d \mid n} \prod_{P \in A(d,p)} P$) ou version avec q... avec déf $A(n,q)$ + $I(n,q)$ (Dév 2)

Cor60 : $I(n,p) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$, $I(n,p) \underset{+\infty}{\sim} \frac{p^n}{n}$

[FRA] ou [Goz]

Rem61 : $I(n,p) > 0$ dc $\exists$ un polyn. unit. irréd P de d° n dans $\mathbb{F}_p[X]$, $\forall n \in \mathbb{N}^*$.

pas de C) → C) Matrices à coeffs dans un corps fini $q = p^n$, $m \in \mathbb{N}^*$

[PER]

Prop62 : $|GL_m(\mathbb{F}_q)| = \prod_{i=0}^{m-1} (q^m - q^i)$; $|SL_m(\mathbb{F}_q)| = q^{m-1} \prod_{i=0}^{m-2} (q^m - q^i)$

Cor63 : $\forall k \in [\![1; m]\!]$, on a $\frac{\prod_{i=m-k}^{m-1} (q^k - 1)}{\prod_{i=1}^{k} (q^i - 1)}$ ss-ev de $\mathbb{F}_q^m$ de dimension k.

Prop64 : Soit $D_m(\mathbb{F}_q) = \{M \in GL_m(\mathbb{F}_q) \mid M \text{ diagonalisable}\}$. $D_m(\mathbb{F}_q) = \{M \in GL_m(\mathbb{F}_q) \mid M^{q-1} = I_m\}$ (8)

Σ à quoi sert cette partie ?
→ Regarder ce qu'est le code correcteur à la place ? (9)